Cure or Curse? Compliance in Digital Healthcare

CEJ
COMPLIANCE ELLIANCE JOURNAL

Content Curators:
Michele DeStefano (University of Miami School of Law)
Dr. Hendrik Schneider (University of Leipzig Faculty of Law)

ISSN 2365-3353
Volume 4 • Number 2
Fall 2018

Compliance Elliance Journal (CEJ)
Volume 4, Number 2, 2018
ISSN: 2365-3353
This version appears in print and online. CEJ is published twice per year, in spring and fall.

Title: Cure or Curse? Compliance in Digital Healthcare

Content Curators:
Michele DeStefano, University of Miami School of Law and LawWithoutWalls
Dr. Hendrik Schneider, University of Leipzig Faculty of Law

Technical Support:
Hannah Beusch
Hans-Henning Gonska
Dr. Niels Kaltenhäuser

Website: www.cej-online.com

Email: info@cej-online.com

Address:
Taunusstrasse 7
65183 Wiesbaden, Germany

Telephone: +49 0341 / 97 35 220

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

Cure or Curse? Compliance in Digital Healthcare

TABLE OF CONTENTS

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

EDITORIAL

CURE OR CURSE? COMPLIANCE IN DIGITAL HEALTHCARE

Digitization – a term one cannot avoid nowadays. Some even speak of a digital revolution with reference to the industrial revolution more than 200 years ago. And both revolutions are truly comparable in the ways they disruptively change our working and living conditions up to the socio-economic structure.

After addressing aspects of Legal Tech in our last issue, we will focus on the field of healthcare in this fall's edition of CEJ. It is especially in the healthcare sector where digitization is to develop its enormous disruptive potential. Not only will there be new techniques of diagnosis and treatment, but also massive changes to the relationships between physicians and patients, providers and users of healthcare services: "The patient will see you now" – the title of Eric Topols bestselling book is not just a play with words! Everything we thought we knew for sure about the structures of our healthcare system may be put upside down. Needless to say that data generation, processing and usage are gamechangers in this regard. Patient data are the lubricant for a developing healthcare system and keep it running. However, the question remains open whether digitization will empower patients to emancipate and to meet physicians at eye level or whether it will make them even more dependent and vulnerable.

Digital (r)evolution is progressing rapidly and legislators seem to struggle keeping pace. The legal framework for the (digital) healthcare sector is complex and uncertain. It often seems to fail to take the "glocality" of digital health care services into account.

New forms of healthcare – new legal questions: questions concerning contract design, liability, settlement, data generation, compatibility with professional regulations as well as with national and supranational law. A bunch of questions remain to be answered. CEJ aims to put these pieces together in a couple of issues focusing on "E-Health and Telemedicine". This edition is the first one and has been supported by Prof. Dr. Michael Lindemann, who holds the chair for Criminal Law, Criminal Procedure and Criminology at the University of Bielefeld, Germany. In his research, Prof. Lindemann focusses (amongst other) on commercial and medical criminal law as well as on the criminological aspects of white collar and corporate crimes. Prof. Lindemann is also coordinator of the Bielefeld Center for Healthcare Compliance (BCHC).

The edition features first-rate articles by specialists in the field of healthcare and data security. Apart from that we will face some classical compliance topics and last but not least CEJ Founder Michele DeStefanos new book *Legal Upheaval* will be introduced and reviewed.

We hope you enjoy our fall edition! Because no matter whether you appreciate the recent developments or find them even frightening – the radical changes digitization causes in the health care industry do affect each of us and are not to be ignored.

With our best regards,

Michele DeStefano, Hendrik Schneider & Michael Lindemann
Founder and Content Curators of CEJ

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

BLOCKCHAIN IN EU E-HEALTH – BLOCKED BY THE BARRIER OF DATA PROTECTION?

Ulrich M. Gassner

AUTHOR

Ulrich M. Gassner is a professor at the Law School of the University of Augsburg, Germany, and the founding director of the Center for E-Health Law. His main research interests include health law, pharmaceutical law, constitutional, and administrative law and data protection law. His publication list counts more than hundred books and articles related to health law. He also is co-editor of several law journals and book series. Furthermore, Ulrich M. Gassner advises private and public clients on a broad range of health law matters, with a focus on e-health law and pharmaceutical law.

ABSTRACT

Compliance with data protection requirements is always a tricky business and even more intricate when it comes to cutting-edge technologies such as distributed ledger technology (DLT), better known as Block Chain Technology (BCT). These difficulties increase even more when the personal data concerned is accorded a special level of protection, as is the case with health data. The following article aims to describe and analyze the legal issues associated with this scenario. The focus here is on the European Union's (EU) General Data Protection Regulation (GDPR)[1], which took effect on May 25, 2018. Furthermore, the functionality of BCT and its possible fields of application in healthcare will be outlined.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 of 4.5.2016, p. 1).

TABLE OF CONTENTS

I. HYPE OR HOPE?

Block Chain Technology (BCT) has recently been referred to as "the most disruptive tech in decades".[2] Others consider it a fundamental technology that "has the potential to create new foundations for our economic and social systems."[3] In that respect, the Gartner Hype Cycle, introduced in 1995 by the technology analyst firm Gartner, Inc., proposes useful guidance. The hype cycle model traces the evolution of technological innovations in terms of expectations or visibility of the value of the technology. It explains the path that technologies generally take, from their initial introduction into the market until their eventual maturation into useful components of broader solutions.[4] According to this model, the five key phases of a technology's life cycle are:

(1) Innovation Trigger: A potential technology breakthrough kicks things off. Early proof-of-concept stories and media interest trigger significant publicity. Often no usable products exist and commercial viability is unproven.
(2) Peak of Inflated Expectations: Early publicity produces a number of success stories – often accompanied by scores of failures.
(3) Trough of Disillusionment: Interest wanes as experiments and implementations fail to deliver. Producers of the technology shake out or fail. Investments continue only if the surviving providers improve their products to the satisfaction of early adopters.
(4) Slope of Enlightenment: More instances of how the technology can benefit the enterprise start to crystallize and become more widely understood. Second- and third-generation products appear from technology providers. More enterprises fund pilots; conservative companies remain cautious.
(5) Plateau of Productivity: Mainstream adoption starts to take off. Criteria for assessing provider viability are more clearly defined. The technology's broad market applicability and relevance are clearly paying off.

In a recent study based on data from more than 3,100 CIOs from 98 countries Gartner sees BCT as a whole at the Peak of Inflated Expectations phase, whereas blockchain in e-health is still assigned to the phase of Innovation Trigger,[5] as most initiatives are still in alpha or beta stage. But without any doubt BCT in e-health will rapidly ascend to the

---

2 Lucas Mearian, *What is blockchain? The most disruptive tech in decades*, COMPUTERWORLD (May 31, 2018 1:35 PM PT), https://www.computerworld.com/article/3191077/security/what-is-blockchain-the-most-disruptive-tech-in-decades.html?page=2 (last visited Aug. 20, 2018, 01:30 PM).

3 MARCO IANSITI & KARIM R. LAKHANI, THE TRUTH ABOUT BLOCKCHAIN, IN HBR'S 10 MUST READS 2018: THE DEFINITIVE MANAGEMENT IDEAS OF THE YEAR FROM HARVARD BUSINESS REVIEW 159 (2018).

4 See for a critical analysis, Martin Steinert & Ozgur Dedehayir, *The hype cycle model: A review and future directions*, 108 TECHNOL. FORECAST. SOC. CHANGE 28 ff. (July 2016).

5 GARTNER (ED.), BLOCKCHAIN STATUS 2018: MARKET ADOPTION REALITY (2018), quoted by: Christiane Pütter, *Erwartungen an Blockchain zurückstutzen*, CIO (June 22, 2018), https://www.cio.de/a/erwartungen-an-blockchain-zurueckstutzen,3580750 (last visited Aug. 20, 2018, 01:30 PM).

Peak of Inflated Expectations phase. Consequently, there is some evidence that the excitement around using BCT in healthcare is growing.[6] An example of this may be the somewhat evangelical fervor of some over-enthusiastic early adopters especially in the U.S., but also in other tech-savvy countries. Others argue that BCT in healthcare is all hype – a technological hammer looking for a nail – and that the complexities of health information could prevent its practical use.[7] However, most people seem to have recognized that, when the dust of the hype clears, BCT may have a significant role to play as a main component of the digital transformation of the healthcare sector. According to the Gartner study, this technology is upwards of only ten years from mainstream adoption. Therefore, it comes as no surprise that many advocates are already pointing to BCT's potential to revolutionize healthcare in terms of the secure and efficient sharing of health data, of fostering patient empowerment, etc.[8]

Even good old Europe has jumped on the bandwagon. Within the framework of EU's Horizon 2020 research and innovation program, the research project My Health My Data (MHMD) has been funded 3,455.190 EUR (ca. 4 mio. USD). It aims to use BCT to enable medical data to be stored and transmitted safely and effectively. The MHMD project is centered on the connection between organizations and individuals, encouraging hospitals to start making anonymized data available for open research, while prompting citizens to become the ultimate owners and controllers of their health data. For these purposes, it will create a platform relying on BCT.[9]

---

6 See, e.g., William Gordon, Adam Wright & Adam Landman, *Blockchain in Health Care: Decoding the Hype*, NEJM Catalyst (February 9, 2017), https://catalyst.nejm.org/decoding-blockchain-technology-health/ (last visited Sept. 17, 2018, 10:05 AM).

7 Id.

8 See, e.g., CHRISTINA CZESCHIK & RATKO STAMBOLIJA, A QUICK GUIDE TO BLOCKCHAIN IN HEALTHCARE, 18 et seq. and passim (2nd ed. 2018); PETER B. NICHOL, THE POWER OF BLOCKCHAIN FOR HEALTHCARE: HOW BLOCKCHAIN WILL IGNITE THE FUTURE OF HEALTHCARE, 14 et seq. (2017); AXEL SCHUMACHER, BLOCKCHAIN & HEALTHCARE STRATEGY GUIDE 2017: REINVENTING HEALTHCARE: TOWARDS A GLOBAL, BLOCKCHAIN-BASED PRECISION MEDICINE, 2 et seq. (2017); Devon S. Connor-Green, *Blockchain in Heathcare Data*, 21 INTELL. PROP. & TECH. L. J. 93, at 106-07 (2017); Leslie Mertz, *(Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution*, 9(3) IEEE PULSe 4 (2018); Juan M. Roman-Belmonte, *Hortensia De la Corte-Rodriguez & E. Carlos Rodriguez-Merchan, How blockchain technology can change medicine*, 130 POSTGRAD MED 420 (2018); Gordon, Wright & Landman, supra note 5; David Randall, Pradeep Goel & Ramzi Abujamra, *Blockchain Applications and Use Cases in Health Information Technology*, 8 J HEALTH MED INFORMAT 276 (2017); Stanislaw P. Stawicki, Michael S. Firstenberg & Thomas J. Papadimos, *What's new in academic medicine? Blockchain technology in health-care: Bigger, better, fairer, faster, and leaner*, 4(1) INT J ACAD MED 1 (2018); Viola Hoffmann, *Blockchain technology as an opportunity for more transparency and self-determination*, GESUNDHEITSINDUSTRIE BW (January 15, 2018), https://www.gesundheitsindustrie-bw.de/en/article/news/blockchain-technology-as-an-opportunity-for-more-transparency-and-self-determination/ (last visited Sept. 17, 2018, 10:40 AM).

9 My health, my data - A New Paradigm in Healthcare Data Privacy and Security, (last visited Oct. 10, 2018, 10:40 AM) http://www.myhealthmydata.eu/.

II. HOW DOES BCT WORK?

BCT was the brainchild of the Bitcoin creator(s) acting under the pseudonym Satoshi Nakamoto. Bitcoin saw the light of day in a paper of 2008 and was conceptualized as a decentralized, cryptographically empowered currency framework for financial interactions without an intermediary. However, while cryptocurrencies are part of the blockchain phenomena, BCT is not limited to cryptocurrencies. Rather, BCT has the potential to restructure economic and social systems and even create new foundations in them. So far there have also been use cases for personal identity verification, land-title deeds, intellectual property ownerships, public and financial records, and digital (or "smart") contracts that automatically execute when certain pre-defined conditions are met. From a technological point of view a smart contract means a piece of software that controls and/or documents or even effects a legally relevant activity.
In general, the blockchain may be defined as a public (distributed) ledger which works like a log by keeping a growing list of records, called "blocks", of all transactions in a chronological order, secured by an appropriate consensus mechanism and providing a record that is, at least in principle,[10] immutable. BCT is also often considered as a decentralized database using the peer-to-peer principle. As opposed to a traditional (e.g., relational) database, there is no central ownership. Instead, information is managed through the consensus of the network members, who cooperate to decide what gets added to the database. In sum, the exceptional characteristics of BCT include immutability, irreversibility, decentralization, persistence and anonymity.[11]

The three main components of BCT are:

(1) A peer-to-peer computer network,
(2) a network protocol, and
(3) a consensus mechanism.[12]

Basically, the peer-to-peer network can be public (unpermissioned, open) or private (permissioned[13], closed). The main differences between these two types are as follows:

---

10 Cf., e.g., Gideon Greenspan, *The Blockchain Immutability Myth*, MULTICHAIN (May 4, 2017), https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/ (last visited Sept. 17, 2018, 10:40 AM).

11 Cf., e.g., Dylan Yaga, Peter Mell, Nik Roby & Karen Scarfone, *Draft Nistir 8202: Blockchain Technology Overview*, NIST (January 2018), https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf (last visited Sept. 17, 2018, 10:40 AM); ARSHDEEP BAHGA & VIJAY MADISETTI, BLOCKCHAIN APPLICATIONS. A HANDS-ON APPROACH, 20-23 (2017); Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, & Gautam Das, *Everything you Wanted to Know about the Blockchain*, 7(4) IEEE CONSUMER ELECTRONICS MAGAZINE 6 (2018).

12 CZESCHIK & STAMBOLIJA, supra note 8, at 10 et seq.

13 Furthermore, permissioned blockchains which allow anyone to join a network once identity and role are defined have to be differentiated from private blockchains, which allow only known or internal nodes to participate in the network.

(1) Control over the network. Public chains are controlled by the wide community of core developers, users, and miners or validators. In turn, private blockchains are governed out by a specific group of people or institutions.
(2) Consensus mechanism (see below).
(3) Application. While public chains are mostly used for payments (as seen in Bitcoin) or as a platform for decentralized applications' development (as seen in Ethereum), almost all private chains are used for solving specific business tasks.[14] Accordingly, most healthcare BCT projects are based on private blockchains.[15]

Each computer in a specific network is called a "node". If everything is running per protocol, each node should have a copy of the entire ledger, which is sort of a local database. This means if one node disconnects or goes down, no data is lost and the ledger's consistency will be kept.
The underlying principle of any transaction is that of public/private key encryption in order to generate digital signatures. A user has two keys: a public key to encrypt data and a private key to decrypt them. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash). And unless one of the parties to the transaction decides to link a public key to a known identity it is impossible to match transactions to individuals or organizations. Although anyone can see all the transactions on the blockchain no personal information is linked to them or made public. This allows any party to validate the integrity of the transaction ledger without violating the privacy of the parties involved in the transaction.
All transactions are verified by a consensus mechanism which is a set of rules utilized by the network to verify each transaction and confirm the current state of the blockchain. In most cases, public chains use Proof-of-Work (PoW) systems, in which so-called "miners" solve cryptographic puzzles to "mine" a block in order to add to the blockchain. This process requires an immense amount of energy and computational usage. When a miner solves the puzzle, they present their block to the network for verification. Verifying whether the block belongs to the chain or not is an extremely simple process. In contrast, private blockchains mostly use well-known and established consensus algorithms with authentified participants such as modified Proof-of-Authority (PoA). In PoA-based networks, transactions and blocks are validated by approved accounts, known as validators, who replace miners. However, as there is no "perfect" consensus mechanism, the search for a truly decentralized consensus mechanism is still going on.[16]
In sum, the result of BCT is an expansive and distributed source of truth built not from trust, but through cryptographically enforced consensus. As its most important attribute can be considered its immutability: once something has been added to the blockchain, it

14 See, e.g., Ivan Grekov, *Is the Right to Be Forgotten a Real Problem for Blockchain?*, LAWLESS.TECH (Apr. 16, 2018), https://lawless.tech/is-the-right-to-be-forgotten-a-real-problem-for-blockchain/ (last visited Sept. 17, 2018, 10:20 AM).

15 CZESCHIK & STAMBOLIJA, supra note 8, at 10.

16 CZESCHIK & STAMBOLIJA, supra note 8, at 11; see also, e.g., Basic Primer: Blockchain Consensus Protocol, Blockgeeks, https://blockgeeks.com/guides/blockchain-consensus/ (last visited Sept. 17, 2018, 10:20 AM).

is permanently stored in a large number of computers.[17]

III. HOW CAN BCT BE APPLIED TO HEALTHCARE?

Realized and probable applications of BCT in healthcare can be divided into eight main areas, namely electronic health records (EHR) management and interoperability, biomedical research, medication planning and management, revenue cycle management (RCM), procurement policies and supply chain management (SCM), internet of medical things (IoMT), health professions education, and international medicine and global health.

A. EHR management and interoperability

Most healthcare systems suffer from the siloing of patients' health data and a lack of interoperability between different domains. Several current health record systems – in the U.S., for example, as well as in most European countries with the exception of Estonia[18] – are composed of an enormous number of disconnected databases. Health records are usually spread across various institutions, health care providers, and suppliers that often use incompatible databases, without full access to a shared patient database. This lack of interoperability leads to enormous inefficiencies.[19]
BCT would provide the ability to replace these disparate systems with an integrated system that, with the use of smart contracts and fully auditable history, enables peer-to-peer interoperability among participants (such as physicians, medical institutions, insurance companies, and pharmacies) within transactions.[20] Using BCT as a data management tool would be especially useful for the implementation of so-called integrated healthcare models, in which the stationary and ambulatory sectors need to exchange information to create an efficient and agreeable patient journey.[21] Instant access to an agreed set of data about a patient would also mean better data for better care in acute, life-threatening situations

17 WRIGHT & LANDMAN, supra note 6.

18 This small EU member state was the first country to implement a blockchain into their electronic healthcare record (EHR) system with the collaboration of a local company named Guardtime, using keyless signature infrastructure (KSI), Danielle Siarri, The potential of blockchain in HER, Oct. 6, 2017, https://www.himss.eu/himss-blog/potential-blockchain-ehr [last visited Oct. 18, 2018, 10:40 AM]; Johnathon Marshall, *Estonia prescribes blockchain for healthcare data security*, PWC (March 16, 2017), http://pwc.blogs.com/health_matters/2017/03/estonia-prescribes-blockchain-for-healthcare-data-security.html (last visited Sept. 17, 2018, 10:10 AM); see also the official website https://e-estonia.com/blockchain-healthcare-estonian-experience/.

19 CZESCHIK & STAMBOLIJA, supra note 8, at 18.

20 Randall, Goel & Abujamra, supra note 8; Igor Radanović & Robert Likić; *Opportunities for Use of Blockchain Technology in Medicine*, APPL HEALTH ECON HEALTH POLICY (July 18, 2018), doi: 10.1007/s40258-018-0412-8; Arlindo Flavio da Conceição, Flavio Soares Correa da Silva, Vladimir Rocha, Angela Locoro & João Marcos Barguil, *Electronic Health Records using Blockchain Technology*, CORNELL UNIVERSITY LIBRARY (April 26, 2018, https://arxiv.org/abs/1804.10078 (last visited Sept. 17, 2018, 10:10 AM).

21 CZESCHIK & STAMBOLIJA, supra note 8, at 34.

and for better treatment of chronic longer-term conditions (e.g., diabetes[22]). Patients could be treated more quickly and in a more targeted way. As a result, for example, the duplication of examinations or treatments would be prevented, ultimately increasing efficiency.[23] Furthermore, sharing the ledger among the participants would bring transparency to the whole process of treatment, from monitoring drug compliance to facilitating cost controls.[24] In addition to offering interoperability, blockchain transactions would also have the advantage of being cryptographical and irrevocable, thus ensuring privacy across parties[25] and reducing fraud.[26] Moreover, in the BCT environment, the patient (or his relatives) would be able to designate by whom the data can be accessed (and at what level of access) by the use of keys that only users would be able to dispose of (either private or public).
The key management and the access control could be encoded in a chaincode, thus ensuring patients' autonomy and self-determination.[27]

B. Biomedical research

Lack of reproducibility, related to a wide range of scientific misconduct aspects, from errors to frauds, compromises the outcomes of clinical studies and undermines research quality. BCT offers the chance to tackle this huge medical challenge for contemporary biomedical research. Study data would be time stamped and publicly more transparent than now. All plans, consents, protocols, and outcomes could be stored in a blockchain. Furthermore, smart contracts could be used to link together several phases of a clinical study.[28] Additionally, as a more general factor, the application of BCT could bring about the access to a large pool of anonymous and encrypted medical data that could be used for personalized drug development and epidemiological studies.[29]

---

22 Simon Lebech Cichosz, Mads Nibe Stausholm, Thomas Kronborg, Peter Vestergaard & Ole Hejlesen, *How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept*, J DIABETES SCI TECHNOL (July 26, 2018), doi: 10.1177/1932296818790281.

23 Hoffmann, supra note 8.

24 Alevtina Dubovitskaya, Zhigang Xu, Samuel Ryu, Michael Schumacher & Fusheng Wang, *How Blockchain Could Empower eHealth: An Application for Radiation Oncology, in:* Data Management and Analytics for Medicine and Healthcare 3, 4-5 (Edmon Begoli, Fusheng Wang & Gang Luo eds. 2017).

25 CZESCHIK & STAMBOLIJA, supra note 8, at 35; Randall, Goel & Abujamra, supra note 8.

26 Randall, Goel & Abujamra, supra note 8.

27 CZESCHIK & STAMBOLIJA, supra note 8, at 35-36; Dubovitskaya, Xu, Ryu, Schumacher & Wang, supra note 24, at 5; Radanović & Likić, supra note 20; Randall, Goel & Abujamra, supra note 8; Hoffmann, supra note 8.

28 Mehdi Benchoufi & Philippe Ravaud, *Blockchain technology for improving clinical research quality*, 18 TRIALS 335 (2017); Dubovitskaya, Xu, Ryu, Schumacher & Wang, supra note 24, at 5; Radanović & Likić, supra note 20.

29 Radanović & Likić, supra note 20.

C. Medication planning and management

Without any doubt, medication reconciliation is one of the most important tasks related to quality of care and patient safety. Using appropriate patient safety algorithms via BCT, medication errors, contraindications, and medication prescriptions could be reconciled near-instantaneously - without the need for time-consuming medication reconciliation processes.[30]

D. Revenue cycle management (RCM)

BCT can help hospitals and health systems to improve the performance of revenue cycle management by reducing denials and boosting patient collections because it allows payers, providers, and financial institutions to share information via private distributed ledgers.[31]

E. Procurement policies and supply chain management (SCM)

BCT could considerably improve procurement policies since it would ensure that the supply of goods is transparent, verifiable, and more efficient. Suppliers could be more easily controlled and, if necessary, held accountable for the quality of their products. The logistics of pharmaceutical and medical device manufacturers could profit from BCT especially as there is a high risk of substandard or counterfeited products entering the supply chain. By introducing smart contracts, checks and transactions could be carried out automatically. In transactions, in which no conflicts are detected, even payments might be automatized.[32]

F. Internet of medical things (IoMT)

IoMT refers to the collection of medical devices and applications that connect to healthcare IT systems through online computer networks. Medical devices equipped with WiFi, Bluetooth, or other interfaces allow the machine-to-machine communication that is the basis of IoMT. The cybersecurity of the connected medical devices and the vulnerable sensitive data that passes through the IoMT could be ensured by BCT.[33]

---

30 CZESCHIK & STAMBOLIJA, supra note 8, at 20 et seq.; Stawicki, Firstenberg & Papadimos, supra note 8.

31 Kelly Gooch, *4 ways to improve RCM with blockchain*, Becker's Hospital CFO Report (March 28, 2018), https://www.beckershospitalreview.com/finance/4-ways-to-improve-rcm-with-blockchain.html (last visited Sept. 17, 2018, 10:10 AM).

32 CZESCHIK & STAMBOLIJA, supra note 8, at 23; Stawicki, Firstenberg & Papadimos, supra note 8.

33 CZESCHIK & STAMBOLIJA, supra note 8, at 23-4; Bernard Marr, *Blockchain And The Internet Of Things: 4 Important Benefits Of Combining These*, Forbes (Jan 28, 2018, 12:28 AM), https://www.forbes.com/sites/bernardmarr/2018/01/28/blockchain-and-the-internet-of-things-4-important-benefits-of-combining-these-two-mega-trends/#50249c9a19e7 (last visited Sept. 17, 2018, 10:10 AM); Matthew Warner, Two Mega Trends Blockchain Technology to Secure Internet of Medical Things, Chain-Finance (Aug. 15, 2017, 1:35 AM),

G. Health professions education

Novel methods of health professions education have often been criticized for their lack of the ability to ascertain the origin, validity, and accountability of the knowledge that is created, shared, and acquired. If based on BCT it will potentially allow improved tracking of content and the individuals who create it, quantify educational impact on multiple generations of learners, and build a relative value of educational interventions.[34] Additionally, records on this digital ledger could continue to grow during the professional life of the physician, archiving attended conferences, written articles, and rates of successful treatments.[35]

H. International medicine and global health

In the area of academic international medicine and global health, blockchain-enabled assessment systems could lead to an alignment of effort allocation between settings (e.g. national and international), the immediate provision of much-needed assistance to low-resource environments, and the reduction of brain-drain that plagues areas in greatest need for healthcare delivery. In terms of its potential impact on the current global healthcare system, BCT could be one of the key components of ensuring both stability and sustainability in the future.[36]

IV. BCT VS. DATA PROTECTION?

A. Patient empowerment by BCT and privacy rules?

As of now, health information is widely controlled by insurance companies and funds, hospitals, doctors, and other intermediaries who, while claiming trustworthiness, are in a position to exploit that trust within essentially asymmetric power structures. BCT could reduce the role of these intermediaries, thus shifting the power balance in favor of the patients. It is capable of putting patients at the center of their health data and enabling data transactions not only to be secure, but also accessible and under the control of the individual patient. If implementing BCT can successfully re-distribute the control of health data back to individuals this could make individual access rights obsolete.[37]

---

http://www.chain-finance.com/2017/08/15/blockchain-technology-to-secure-internet-of-medical-things/ (last visited Sept. 17, 2018, 10:10 AM).

34 Eric Funk, Jeff Riddell, Felix Ankel & Daniel Cabrera, *Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education*, Acad Med. (June 12, 2018), doi: 10.1097/ACM.0000000000002326; Radanović & Likić, supra note 20.

35 Radanović & Likić, supra note 20.

36 Stawicki, Firstenberg & Papadimos, supra note 8.

37 Cf. Connor-Green, supra note 8, at 99, 106-07, referring to the U.S. legal situation.

However, BCT cannot solve all trust and privacy concerns surrounding health data protection. Therefore, it has been proposed that the U.S. federal regulation governing healthcare data privacy, the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[38] should be supplemented with stricter rules in line with the model of the GDPR[39]. Coupled with BCT, it would affirm a paradigm shift in the US-American legal landscape in terms of data ownership.[40] The GDPR, however, does not explicitly refer to the intrinsically problematic concept of personal data ownership. Rather, it follows merely from the wording of sentence 2 of its Recital[41] 7, "Natural persons should have control of their own personal data", that data subjects should be in control of their personal data.

The regulation paints the term "personal data" with a very broad stroke. It is defined in Article 4(1) GDPR as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person". It is well established that personal data that has been encrypted or hashed still qualifies as personal data within this definition as it is merely pseudonymized and not irreversibly anonymized.[42] It follows that not only personal data but also public keys used in BCT qualify as personal data, just like data relating to a natural person that is hashed to the chain.[43] As a consequence, cryptographically modified health data stored, e.g., on a distributed ledger of an integrated EHR, in addition to public keys, are subject to the GDPR.

Furthermore, as opposed to the narrower approach of the HIPAA Privacy Rule[44] all individuals, organizations, and companies that are either "controllers"[45] or "processors"[46]

---

38 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

39 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 of 4.5.2016, p. 1).

40 Connor-Green, supra note 8, at 99.

41 Recitals are important because they are used by the Court of Justice of the European Union (CJEU) and other EU institutions in order to interpret any Directive or Regulation.

42 MICHÈLE FINCK, BLOCKCHAINS AND DATA PROTECTION IN THE EUROPEAN UNION 10-11, SSRN (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322 (last visited Sept. 17, 2018, 4:20 PM); cf. further Article 29 Working Party, Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN, 20; but see BLOCKCHAIN BUNDESVERBAND, BLOCKCHAIN, DATA PROTECTION, AND THE GDPR 4 (2018).

43 FINCK, supra note 42, at 12-14.

44 See, e.g., Connor-Green, supra note 8, at 104-05.

45 A "data controller" is a party that determines the purposes and means of the processing of personal data, see Article 4(7) of the GDPR.

46 A "data processor" is a party that processes personal data on behalf of the controller, see Article 4(8) of the GDPR.

of personal data are covered by the GDPR. This does not mean that the regulation applies to all processing of personal data of EU citizens or residents, as often incorrectly stated. Rather, pursuant to Recital 80 of the GDPR, its territorial scope includes the processing of personal data of someone "in the Union" by data controllers or processors outside, "where the processing activities are related to the offering of goods or services" to that person, even if they do not require payment. According to Recital 23 of the GDPR, the appropriate test is based on whether the organization "envisages" offering goods and services, not on whether it does in fact offer, supply, or simply obtain personal data.[47]
The goal of effective control by data subjects is accomplished by, inter alia, requiring explicit and informed consent for the collection and use of data (Articles 6(1)(1)(a) and 7 GDPR) and imposing stiff fines on data controllers or processors for non-compliance (Article 83 of the GDPR). One of the cores of the regulation is formed by eight fundamental and dispositive rights of the data subjects that are outlined below.

(1) The right to be informed (Articles 13 and14 of the GDPR): A data subject has the right to know how his or her data will be collected, processed, and stored, and for what purposes.
(2) The right to access information (Article 15 of the GDPR): A data subject has the right to know how his or her data has been collected, processed, and stored, what data exists, and for what purposes.
(3) The right to rectification (Article 16 of the GDPR): A data subject has the right to have inaccurate or incomplete data corrected.
(4) The right to erasure ("the right to be forgotten") (Articles 17 and 19 of the GDPR): A data subject has the right to have personal data permanently deleted without the need for a specific reason as to why he or she wishes to discontinue the data storage.
(5) The right to restriction of processing (Article 18 of the GDPR): A data subject has the right to block or suppress his or her personal data being processed or used.
(6) The right to data portability (Article 20 of the GDPR): A data subject has the right to transfer personal data from one data controller to another in a safe and secure way and in a commonly used and machine-readable format.
(7) The right to object to processing of personal data (Article 21 of the GDPR): A data subject has the right to object to being subject to public authorities or companies processing their data without explicit consent and to stop his or her personal data from being included in direct marketing databases.
(8) The right to not be subject to automated decision-making (Article 22 of the GDPR): A data subject has the right to demand human intervention, rather than having important decisions made solely by algorithm.

So, at first sight, there may be a case for supplementing the HIPAA by selected features

47 See, e.g., Pascal Schumacher, *Territorial cope of application of the GDPR – Change from the principle of territoriality to effects doctrine*, *in* New European General Data Protection Regulation. A Practitioner's Guide 38-39 (Daniel Rücker & Tobias Kugler eds., 2018); PAUL VOIGT & AXEL VON DEM BUSSCHE, THE EU GENERAL DATA PROTECTION REGULATION (GDPR), 26-29 (2017).

of the GDPR in order to improve health data privacy. But when looking at some of the data subject's rights mentioned above, the question may arise whether a decision has to be made between using BCT and applying GDPR-standards. For example, the right of erasure appears to be particularly at odds with the immutable nature that is at the core of BCT.[48] Consequently, the issue whether BCT and GDPR can co-exist, is to be examined in more detail below.

B. Does the GDPR block BCT?

1. Systemic tension

Arguably, BCT and the GDPR are profoundly incompatible even at a conceptual level as the data protection mechanisms developed for centralized data silos cannot be easily reconciled with a decentralized method of data storage and protection. However, personal data in a blockchain system that is encrypted or hashed is still subject to the GDPR and public keys used in BCT surroundings are qualified as personal data under EU law.[49] Herefrom results not only a risk that the GDPR renders the operation of blockchains unlawful. Rather, this tension reveals also a clash between the goals of the protection of privacy on the one hand, and the promotion of innovative technology on the other hand.[50] However, due to the different construction of unpermissioned and permissioned blockchains, the latter being dominant in healthcare, it is obvious that the latter cause minor difficulties from the point of view of data protection. In addition, technical solutions that can contribute to BCT's data protection compliance are feasible or have already been implemented. This is often overlooked in the sometimes quite simplistic public discussion.[51] We will turn to these issues below.

2. Personal data

While BCT allows for personal data to be stored in the same way as in a database, personal can also be stored "off chain" in a separate database and only linked to the blockchain via private and public cryptographic keys. Consequently, GDPR compliance can be ensured

48 See, e.g., Samuel Martinet, *GDPR and Blockchain: Is the New EU Data Protection Regulation a Threat or an Incentive?*, Cointelegraph (May 27, 2018), https://cointelegraph.com/news/gdpr-and-blockchain-is-the-new-eu-data-protection-regulation-a-threat-or-an-incentive (last visited Sept. 17, 2018, 10:10 AM).

49 See supra section IV.

50 Cf. FINCK, supra note 42, at 1-2, 28-29; cf. also Anne Toth, *Will GDPR block Blockchain?*, World Economic Forum (May 24, 2018), https://www.weforum.org/agenda/2018/05/will-gdpr-block-blockchain/ (last visited Sept. 17, 2018, 10:10 AM).

51 See, e.g., Gyula Pal, *The GDPR blockchain blind-spot: Regulating data and everything else*, IBM (Jun 26, 2018), https://www.ibm.com/blogs/blockchain/2018/06/the-gdpr-blockchain-blind-spot-regulating-data-and-everything-else/ (last visited Sept. 18, 2018, 01:15 AM); Toth, supra note 50

in that respect.[52] This would be the case, for example, if the EHR themselves continue to be stored in hospital databases, i.e., off the chain. However, such a workaround has the disadvantage that the benefits of transparency and data control with BCT are reduced. Thus, paradoxically, in this context the application of the GDPR leads to a result that is at odds is with its explicit goal that "natural persons should have control of their own personal data" (Recital 7).[53]
Unlike transactional data, public keys cannot be moved off-chain as they are quintessential components of the BCT. Different promising work-arounds have been developed recently, but it is difficult to say at this stage whether any of these techniques will be considered capable of anonymizing public keys for GDPR purposes.[54]

3. Legal status of participants

As the GDPR was designed in a pre-BCT-world with a clear division of responsibilities between controllers and processors, the legal status of the different participants in blockchain networks is rather ambiguous. Especially public blockchains do not fit cleanly in this model. Namely, nodes cannot be considered data controllers in such a setting as they do not determine the means and purposes of the processing of personal data sent to the network by a third party.[55] When it comes to private blockchains, however, it might still be possible to identify a central intermediary. A governance body may be established to oversee the permissioned network. This governance body could not only function as a data processor if it has influence over the purpose and means of processing within the meaning of Article 4(7) of the GDPR but also as a data controller who collects personal data from individuals serving as a single point of legal contact with the network.[56]

4. Data minimization

An important principle in the GDPR is data minimization. Article 5(1)(c) of the GDPR requires that personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". This principle is profoundly at

---

52 Cf. FINCK, supra note 42, at 11-12; BLOCKCHAIN BUNDESVERBAND, supra note 42, at 4; Andries Van Humbeeck, The Blockchain-GDPR Paradox, TheLedger (Nov. 21, 2017), https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047 (last visited Sept. 18, 2018, 01:15 AM); Lucas Mearian, Will blockchain run afoul of GDPR? (Yes and no), Computerworld (May 7, 2018 3:02 AM PT), https://www.computerworld.com/article/3269750/blockchain/will-blockchain-run-afoul-of-gdpr-yes-and-no.html (last visited Sept. 17, 2018, 10:15 AM); Luke Sayer, *Comment: Can GDPR and blockchain co-exist?*, International Investment (May 4, 2018), http://www.internationalinvestment.net/comment/comment-can-gdpr-and-blockchain-co-exist/ (last visited Sept. 18, 2018, 01:15 AM).

53 Cf. Van Humbeeck, supra note 52.

54 FINCK, supra note 42, at 14-16.

55 FINCK, supra note 42, at 16-17; BLOCKCHAIN BUNDESVERBAND, supra note 42, at 5-6.

56 FINCK, supra note 42, at 16; BLOCKCHAIN BUNDESVERBAND, supra note 42, at 7.

odds with data storage in a blockchain since distributed ledgers are by definition ever-growing creatures accumulating further data with each additional block.[57]

5. The right to rectification

Data subjects' rights under Article 16 of the GDPR imply that a rectification request can be addressed to any or all nodes. Two technical hurdles arise in this context. First, even in a permissioned blockchain – standard in healthcare environments – the data subject will face difficulties to identify any or all of the owners of the nodes. Second, even if the data subject succeeds in submitting a claim under Article 16 GDPR, they are simply unable to change any of the encrypted data stored in blocks due to their immutable nature. Again, an off-chain solution may operate as a legal loophole in that respect.[58]

6. The right to access information

With respect to Article 15 of the GDPR similar practical difficulties arise. Controllers do not know what personal data is stored on the blockchains, since they normally handle only the encrypted or hashed version. Even if a data subject were successful in contacting the owner of a node, the latter would not be able to verify whether the personal data of a data subject has been processed. Off-chain storage can again facilitate GDPR compliance in relation to transactional data but not public keys.[59] This is all the more true when a governance body is established to oversee the permissioned network.

7. The right to erasure

According to Jan Philipp Albrecht, the former member of the European Parliament who shepherded the GDPR through the legislative process, the administratively easy exercise of the right to be forgotten "is where blockchain applications will run into problems and will probably not be GDPR compliant."[60] It is however common ground that the right to be forgotten cannot be straightforwardly applied to BCT, as immutability is one of the essential features of blockchains.[61] However, the insight has grown that there is no such thing as perfect immutability in blockchains. For instance, it is easy to undermine if all the participants in a chain decide to do so together.[62]

---

57 FINCK, supra note 42, at 20-21.

58 Cf. id. at 21-22.

59 Id. at 23 (relating to public blockchains).

60 Quoted in David Meyer, *Blockchain technology is on a collision course with EU privacy law*, The Privacy Advisor (Feb. 27, 2018), https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/ (last visited Sept. 17, 2018, 01:20 AM).

61 FINCK, supra note 42, at 23-24; Grekov, supra note 14.

62 Greenspan, supra note 10; see also Grekov, supra note 14.

Furthermore, the principle of immutability can be circumvented by an off-chain or similar solutions. Personal data which is recorded in a referenced encrypted and modifiable database as opposed to the blockchain itself, may be deleted in line with Article 17 of the GDPR.[63]
With respect to public keys, GDPR compliance is again more difficult to reach. Whether any of the several solutions that have been developed up to now can satisfy GDPR requirements remains to be seen.[64] Notwithstanding that, it seems to be worth mentioning that certain implementing acts of the EU member states have already directed themselves towards a softer version of the right to erasure. For instance, Section 35(1) of the German Federal Data Protection Act[65] provides that the data subject shall not have the right to erasure and the controller shall not be obligated to erase personal data if the "erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage and if the data subject's interest in erasure can be regarded as minimal".[66]

C. Does BCT support the GDPR

Despite the tension between technology and law outlined above, it comes not totally as a surprise that BCT is being increasingly considered as a mechanism to help control the use of personal data under the GDPR.[67] The reason is that both initiatives are aligned on the principles of secured and self-sovereign data.[68] A prominent example of this coincidence are the guiding principles of data protection by design and data protection by default. Article 25(1) of the GDPR requires data protection to be designed into the development of business processes for products and services. Specifically, the controller should have technical, procedural, and organizational measures - such as pseudonymization and encryption - in place in order to meet the requirements of the GDPR. Being based on advanced encryption technologies, BCT can support the implementation of GDPR-compliant solutions which also may be a reason for regulators and courts to look favorably at it.[69]

---

63 FINCK, supra note 42, at 24; CINDY COMPERT, MAURIZIO LUINETTI, & BERTRAND PORTIER , BLOCKCHAIN AND GDPR, IBM WHITE PAPER, 3, (2018), https://public.dhe.ibm.com/common/ssi/ecm/61/en/61014461usen/security-ibm-security-solutions-wg-white-paper-external-61014461usen-20180319.pdf (last visited Sept. 17, 2018, 01:20 AM).

64 FINCK, supra note 42, at 24; but see Grekov, supra note 14.

65 Federal Law Gazette I p. 2097.

66 Cf. FINCK, supra note 42, at 26; BLOCKCHAIN BUNDESVERBAND, supra note 42, at 8.

67 Cf., e.g., COMPERT, LUINETTI, & PORTIER, supra note 63; Mearian, supra note 52.

68 COMPERT, LUINETTI, & PORTIER, supra note 63, at 2.

69 FINCK, supra note 42, at 26, 30-31; COMPERT, LUINETTI, & PORTIER, supra note 63, at 6-7 (hinting at the example of the Estonian EHR system).

V. CONCLUSION AND OUTLOOK

In sum, BCT offers many benefits to patients, health care service providers, hospitals, medical researchers, caregivers, and other healthcare parties. It integrates the healthcare ecosystem by adding accountability and transparency, while preserving privacy and confidentiality.[70] This indicates at least partial concordance with the objectives of the GDPR. Thus, BCT can provide an alternative means of achieving the objectives of the GDPR.[71] Yet it is also equally true that there is a systemic tension between technology and privacy law. And without any doubt, some blockchains in healthcare, as currently designed,[72] are incompatible with the GDPR.

Considering that the GDPR was developed without taking BCT into account, it could at first glance be wise to amend it for blockchains.[73] Such a revision of the GDPR would acknowledge the fact that BCT creates order without law and implements private regulatory frameworks (lex cryptographia).[74] However, for the time being, there are hardly any signs of EU reform initiatives in that respect. The European Parliament's Committee on Industry, Research and Energy (ITRE) passed a resolution outlining the benefits of adopting DLT on May 16, 2018, without explicitly requiring amendments to the GDPR.[75] The ITRE only emphasized that "it is of outmost importance [for] the DLT uses to be compliant with the EU legislation on data protection" and calls on the European Commission and the European Data Protection Supervisor (EDPS) to provide for further guidance on this point. After all, one seems to have recognized the problem that there may be some risk that the EU closes itself off from the future of the internet with respect to BCT. The EU Blockchain Observatory and Forum that has been launched by the Commission with the purpose of mapping key initiatives, monitoring developments, and inspiring common actions held a workshop on June 8, 2018 to examine the clashes and correlations between BCT and GDPR, and to provide, as far as possible, some guidance to technologists, lawyers, entrepreneurs, and citizens in that respect, thus echoing the ITRE's resolution on DLT and BCT. The workshop discussed separately the topics of technical, governance, and legal solutions and came to the positive result that there are only a few questions left unanswered or on which no agreement could be reached. This indicates that the reform of the GDPR is not the silver bullet, especially since the mills of

---

70 Cf., e.g., CZESCHIK & STAMBOLIJA, supra note 8, at 34-38.

71 FINCK, supra note 42, at 29.

72 See for examples and use cases of BCT in the healthcare system CZESCHIK & STAMBOLIJA, supra note 8, at 25-31; NICHOL, supra note 8, at 115-47.

73 Toth, supra note 50.

74 PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE, 5 and passim (2018).

75 European Parliament Committee on Industry, Research and Energy (ITRE), Motion for a resolution on distributed ledger technologies and blockchains: building trust with disintermediation, ITRE/8/10 - 2017/2772(RSP) (Compromise Amendments).

Brussels grind slowly. Rather, it seems to be the order of the day that regulators and officials and BCT parties and developers cooperate towards mutually acceptable solutions such as off-chain storage of personal data and technical work-arounds. Furthermore, the creation of a code of conduct for BCT in accordance with Article 40 of the GDPR might be useful.[76]

Of course, the message that GDPR and BCT can co-exist holds also true for healthcare settings. Consequently, the question may arise what EU initiatives exist specifically for the health sector. The ITRE resolution notes that DLT allows citizens to control and have transparency on their health data, chose which of those data to share, including their use with insurance companies and the wider healthcare ecosystem, but stresses also the necessity to protect the privacy of the sensitive health data.[77] According to the European Commission's communication on "Enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society", published on April 24, 2018, it is intended to monitor the implementation of the GDPR and the eIDAS Regulation[78] with regard to health and to take account of emerging technologies such as blockchain in the context of cybersecurity.[79] That makes sense, as in a decentralized BCT ransomware attacks on hospitals etc. would become more difficult.[80] Furthermore, the Staff Working Document accompanying the Commission's communication expresses the expectation that new emerging cybersecurity solutions building on trusted DLT for protecting the access to personal health data such as BCT could play an essential role if implemented systematically across Europe as part of the national and EU level data and computation infrastructures for personalized medicine.[81] However, this is insufficient in the light of the unsettled legal issues discussed above. Therefore, it remains to be hoped that the Commission, in its announced recommendation on the technical specifications for an EHR exchange format,[82] will take the opportunity to clarify the tension-loaded relationship between BCT and GDPR, thereby creating greater legal certainty.

---

76 BLOCKCHAIN BUNDESVERBAND, supra note 42, at 9.

77 European Parliament Committee on Industry, Research and Energy (ITRE), supra note 75.

78 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257 of 28.8.2014, p. 73).

79 COM(2018) 233 final, 6.

80 Gordon, Wright & Landman, supra note 5; SCHUMACHER, supra note 8, at 4.

81 COMMISSION STAFF WORKING DOCUMENT, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM(2018) 233 final, SWD(2018) 126 final, 41.

82 See COM(2018) 233 final, 7.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

DIGITAL HEALTH REGULATORY GAPS IN THE UNITED STATES

Kirk J. Nahra & Bethany A. Corbin

AUTHORS

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, D.C., where he specializes in privacy and information security litigation and counseling. He is chair of the firm's Privacy Practice and assists companies in a wide range of industries in analyzing and implementing the requirements of privacy and security laws across the country and internationally. He provides advice on data breaches, enforcement actions, contract negotiations, business strategy, research and de-identification issues, and privacy, data security, and cybersecurity compliance. He also works with insurers and health care industry participants in developing compliance programs and defending against government investigations into their practices. Kirk, a Certified Information Privacy Professional (CIPP/US), is a longtime member of the Board of Directors of the International Association of Privacy Professionals, and serves on the Advisory Board for the Health Law Reporter, the Privacy and Security Law Report, and the Health Care Fraud Report. He has held leadership positions with various groups within the American Health Lawyers Association and the American Bar Association Health Law Section. He is rated by Chambers USA in the nation's top-tier of privacy attorneys. Kirk can be reached at: E-mail: knahra@wileyrein.com; Phone: (202) 719-7335; Twitter: @KirkJNahrawork.

Bethany A. Corbin is a complex litigation and regulatory compliance attorney with Wiley Rein LLP in Washington, D.C. She represents health care, pharmaceutical, telecommunications, and technology clients in judicial and administrative proceedings. She is a Certified Information Privacy Professional (CIPP/US) and provides strategic advice to health care organizations concerning privacy and cybersecurity. In December, Bethany will obtain her Health Care LL.M. from Loyola University of Chicago, where she has focused her studies on the intersection of health care and technology, including the Internet of Medical Things. Bethany currently serves as the Young Lawyer Representative to the Cybersecurity and Data Privacy General Committee of the Tort, Trial, and Insurance Practice Section of the American Bar Association. Bethany can be reached at: E-mail: bcorbin@wileyrein.com; Phone: (202) 719-4418; Twitter: @BethanyACorbin.

ABSTRACT

Digital health in the United States is rapidly and continuously evolving to enhance patient care and revolutionize health care delivery. This technology offers substantial promise to both patients and providers, but lacks a comprehensive regulatory structure to ensure adequate safety and privacy. While the Department of Health and Human Services, the Food and Drug Administration, and the Federal Trade Commission regulate portions of the digital health industry, their oversight is incomplete, with numerous digital health companies falling between the cracks and assuming an unregulated status. This article analyzes the state of digital health legal and regulatory oversight in the United States, discusses how state legislatures and industry organizations have worked to fill existing legal gaps, and presents strategies for encouraging compliance for unregulated entities.

TABLE OF CONTENTS

I. INTRODUCTION

The boundaries and applications of digital health are rapidly evolving. From wearable fitness sensors to ingestible pills to Internet-connected pacemakers and insulin pumps, digital health has the potential to transform the health care sector and revolutionize patient care. The benefits from digital health are undeniable: patients can assume greater responsibility for the management of chronic conditions while accessing medical care at their convenience and in their own homes.[1] Technology-based health care can further reduce the costs of care and help address the physician shortage across America.[2] These benefits are a significant incentive to increase the adoption of mobile and digital technology in the health care industry, and the rate of this adoption is only projected to increase.

While digital health offers substantial promise, it suffers to some extent from a lack of comprehensive regulation. This regulatory gap presents potential concerns both for patients—who may not be provided with appropriate protections—and for the industry, which will see compliance, operational and strategic challenges in designing products that meet with existing standards, potential future regulation, and consumer and regulator expectations. Privacy laws in the United States are sectoral and patchwork in nature, and those related to health care have not been significantly revised to address technological innovation. Privacy and security for digital health applications are therefore in flux, with some subsections of the industry unregulated by federal law. This article analyzes the scope and gaps of health care privacy and security laws in the United States and discusses available privacy and cybersecurity frameworks that exist for unregulated health care actors.

II. WHAT IS DIGITAL HEALTH?

The term digital health, at its most basic, refers to the intersection of health care and the Internet. Digital technologies that fall within this category are broad, and may include mobile health (mHealth), health information technology (HIT), wearable devices, telemedicine, the Internet of Things (IoT), and personalized medicine.[3] While these technologies serve different functions—for example, HIT includes electronic health records and e-prescribing whereas IoT concerns sensors that interact between humans and machines to collect relevant health care data for diagnosis and disease management—they share one

---

1 See U.S. DEP'T HEALTH & HUMAN SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 2 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf (last visited Aug. 20, 2018, 01:30 PM). [hereinafter HHS HIPAA OVERSIGHT REPORT]

2 Jeff Lagasse, *With Physician Shortage Looming, Hospitals Turn to Telehealth Tools*, HEALTHCARE FINANCE (June 1, 2018), https://www.healthcarefinancenews.com/news/physician-shortage-looming-hospitals-turn-telehealth-tools (last visited Aug. 20, 2018, 01:35 PM).

3 Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 (1), ANNALS HEALTH LAW 1, 4 (2017).

fundamental overriding goal: to use technology as a method for improving health care and increase the access and quality of medical services.

The advent and adoption of digital health has the potential to profoundly impact the health care economy over the next several decades. To date, the United States has spent approximately 18% of its Gross Domestic Product on health care every year, and this figure is expected to increase to 20% by 2025.[4] Digital health, however, is simultaneously expected to grow by a compounded annual growth rate of 26% in the upcoming years, and is projected to top $379 billion by 2024.[5] These anticipated technological developments in the health care space may increase pressure to create and implement lower-cost health care solutions and incentivize companies to continue developing digital health products.[6] Significant shifts in the delivery of health care could be witnessed over the next several years.

III. DIGITAL HEALTH RISKS

Although the benefits of digital health are undeniable, concerns exist regarding the privacy and security of data collected through digital technologies. Like all digital platforms, Internet-connected health care devices pose privacy and security risks for their users. First, digital health applications collect and store patient health data, which may contain extremely sensitive information. Without proper security safeguards, this personal data may be unlawfully accessed by unauthorized users, resulting in a breach of personal information. Such a breach not only harms the business and reputation of the digital device manufacturer, but also exposes critically sensitive patient data. There is no shortage of bad actors attempting to access medical data. Indeed, health data is one of the most lucrative objects for sale on the black market, fetching higher prices than social security numbers and financial information.[7] Thus, the traditional data breach risk that is present with any Internet technology is amplified in the health care context due to value-laden sensitive data.

Second, device interoperability and network connectivity bring the possibility for new attack vectors and vulnerabilities.[8] A network hosting interconnected devices exponentially expands its attack surface such that a security flaw or breach in any device operates as a backdoor entry point into the entire system.[9] These digital health devices weaken the

4 Id. at 3.

5 Keith Speights, *What Is Digital Health?*, MOTLEY FOOL (May 9, 2017, 7:04 AM), https://www.fool.com/investing/2017/05/09/what-is-digital-health.aspx (last visited Aug. 20, 2018, 01:37 PM).

6 Tschider, supra note 3, at 4.

7 See generally PRESIDENT'S NAT'L SEC. TELECOMMUNICATIONS ADVISORY COMMITTEE, NSTAC REPORT TO THE PRESIDENT ON THE INTERNET OF THINGS ES-1 (Nov. 19, 2014), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf (last visited Oct. 23, 2018, 01:35 PM).

8 Id. at 7.

9 See id. at 1.

overall security of a medical IT network by their mere presence on the network, and further create access points that must be monitored and evaluated by the organization's technology team. Unauthorized access into a network further has the potential to compromise data integrity, which can negatively impact patient care and treatment plans.

Finally, digital health offers a unique risk that is not present with all Internet-based platforms: bodily harm. Digital health devices that are implanted into a patient's body, such as a cardiac pacemaker, may use the Internet to receive signals or instructions from a health care provider. Hijacking a pacemaker could allow an unauthorized third party to manipulate the device's functionality and cause significant bodily harm or death. This same scenario is present with digital insulin pumps, where device hijacking could alter the dose of insulin a patient receives.

Thus, digital health presents privacy, security, and resiliency risks that must be addressed and mitigated. These risks are increasingly being discussed in public policy circles, with the widespread recognition that technology advances faster than policy. The result is a crucial gap between legal frameworks and technological reality that heightens the security and privacy risks associated with digital health technology.

IV. DIGITAL HEALTH LEGAL & REGULATORY FRAMEWORKS

Digital health in the United States does not exist in an unregulated environment. Rather, the United States has adopted a sectoral approach to privacy that vests regulatory authority for the health care sector with three federal government agencies (in addition to potential regulation in each of the states): The Department of Health and Human Services (HHS), the Food and Drug Administration (FDA), and the Federal Trade Commission (FTC). In terms of privacy and security, HHS's Office for Civil Rights (OCR) plays a dominant role in its enforcement of the Health Insurance Portability and Accountability Act (HIPAA).[10] HIPAA represents the main legal framework addressing privacy and security requirements for the health care industry, and its applicability to digital health technologies is the focus of this article. In addition to HHS, the FDA regulates the efficacy and safety of medical "devices",[11] and has proposed voluntary cybersecurity guidance for connected medical devices.[12] Finally, the FTC has broad non-industry-specific enforcement powers that stem from Section 5(a) of the Federal Trade Commission Act (FTC Act).[13] Pursuant to the FTC Act, the FTC may regulate unfair and deceptive trade practices in or affecting commerce. While the FTC Act does not specifically mention privacy,

---

10 See HHS HIPAA OVERSIGHT REPORT, supra note 1, at 3.

11 Medical Device Overview, U.S. FOOD AND DRUG ADMINISTRATION (last updated Sept. 14, 2018), https://www.fda.gov/forindustry/importprogram/importbasics/regulatedproducts/ucm510630.htm (last visited Aug. 28, 2018, 01:58 PM).

12 See Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, U.S. FOOD & DRUG ADMINISTRATION (Jan. 22, 2016), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf (last visited Aug. 28, 2018, 01:53 PM).

13 See HHS HIPAA OVERSIGHT REPORT, supra note 1, at 3.

the FTC has brought numerous cases under Section 5(a) alleging that companies have engaged in deceptive acts by failing to adhere to their stated privacy policies and procedures. This article next considers the scope and gaps of these regulatory frameworks as applied to digital health technology, and discusses efforts by state legislatures to bridge these gaps.

A. The Health Insurance Portability and Accountability Act: Scope & Applicability

In 1996, Congress passed the Health Insurance Portability and Accountability Act to enhance the portability of health insurance coverage and reduce the administrative costs and burdens associated with health care delivery.[14] Neither of these primary goals were directed at privacy and security—instead, the privacy and security rules that resulted from the HIPAA law were not discussed in any substantive way in the HIPAA statute. Instead, when Congress failed to step in and create a privacy and security law, HHS (later supplemented by the Health Information Technology for Economic and Clinical Health Act (HITECH Act)), created federal regulatory protections for the privacy and security of certain health information in certain settings when held by certain entities—with the scope of these rules defined by the "non-privacy" goals of the HIPAA statute.[15] The HIPAA Privacy Rule sets forth required limitations on the use and disclosure of protected health information (PHI),[16] while the HIPAA Security Rule mandates administrative, technical, and physical safeguards for electronic PHI.[17] Essentially, HIPAA seeks to protect health information by prohibiting disclosures of information that are unlawful or unauthorized, and ensuring that applicable health care entities enact reasonable and appropriate security safeguards for the data they collect or store.

While the scope of HIPAA appears broad, its privacy and security requirements apply only to health care organizations that qualify as "covered entities."[18] A covered entity is any health plan, health care provider, or health care clearinghouse, as those terms are statutorily defined (again, driven by concerns about portability and administrative simplification and not privacy or security).[19] In 2009, the HITECH Act extended HIPAA's provisions to "business associates," which include persons or organizations that perform certain functions on behalf of a covered entity involving the use or disclosure of PHI—essentially, service providers to these covered entities where the services involve individual information.[20] PHI, in turn, is defined as individually identifiable health information

---

14 Kirk J. Nahra, *HIPAA Privacy and Security for Beginners*, WILEY REIN (July 2014), https://www.wileyrein.com/newsroom-newsletters-item-5029.html (last visited Aug. 28, 2018, 01:55 PM).

15 See id.

16 See 45 C.F.R. § 164.502; DEP'T HEALTH & HUMAN SERVS. OFFICE FOR CIVIL RIGHTS, SUMMARY OF THE HIPAA PRIVACY RULE 1 (last revised May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf?language=en (last visited Aug. 28, 2018, 02:05 PM).

17 See 45 C.F.R. §§ 164.308-312.

18 See, e.g., 45 C.F.R. § 164.502.

19 Id. § 160.103; Nahra, supra note 14.

20 See 45 C.F.R. § 160.103.

that a covered entity or its business associate holds or transmits in any form or media.[21] The foundational principle of HIPAA is that a covered entity or business associate may not use or disclose PHI except as either expressly permitted in the Privacy Rule, or as authorized by the patient in writing. A covered entity is only required to disclose PHI in two circumstances: (1) to the patient herself when requested; and (2) to HHS as part of a compliance investigation or enforcement action.[22] A covered entity is permitted—but not required—to disclose PHI without first obtaining the patient's authorization (with presumed consent under the HIPAA Privacy Rule) for the "core" purposes of the health care system—treatment, payment, and performance of health care operations (TPO) (essentially the administrative operations of a health care business).[23] There also are various "public policy" rationales for the use and disclosure of PHI. All other uses and disclosure of PHI not expressly permitted by the Privacy Rule require an individual's written authorization.

B. HIPAA and Digital Health Technology: Assessing the Gaps

Although HIPAA may appear at first blush to be a comprehensive privacy framework for the health care industry, it has significant gaps and limitations when applied to digital health technology.[24] First, HIPAA's protections only extend to digital health actors that qualify as covered entities. When HIPAA was originally drafted, HHS only had authority to create a privacy rule applicable to covered entities such as health care providers and health insurers.[25] This means organizations that do not qualify as covered entities or business associates typically have no obligation to comply with HIPAA's requirements. For example, a company manufacturing a fitness tracker that collects basic health information such as height, weight, and biometric data, would not be subject to HIPAA's regulations because the company provides this product directly to an individual consumer without the involvement of a doctor or health insurer. The company does not provide or pay the cost of an individual's medical care, does not provide medical services, and does not process non-standard data received from another entity into a standardized format (e.g., billing companies, community health management information systems, etc.). In other words, the company is not a covered entity (i.e., it is not a health plan, a health care provider, or a health care clearinghouse). Thus, this company would fall outside the bounds of HIPAA's privacy and security regulations despite the fact that it collects sensitive health data.

---

21 Id.

22 Id. § 164.502; Nahra, supra note 14.

23 45 C.F.R. § 164.502; Nahra, supra note 14.

24 See HHS HIPAA OVERSIGHT REPORT, supra note 1, at 20; Kirk J. Nahra, *What Closing the HIPAA Gaps Means for the Future of Healthcare Privacy*, HITECH ANSWERS (Nov. 9, 2015), https://www.hitechanswers.net/what-closing-the-hipaa-gaps-means-for-the-future-of-healthcare-privacy-2/ (last visited Aug. 28, 2018, 03:14 PM).

25 Nahra, supra note 24.

Second, HIPAA only protects and regulates PHI. PHI refers to individually identifiable health information (including demographic data) that relates to a person's physical or mental health, the provision of health care services to that individual, or payment for health care services, and that identifies the individual or would provide a reasonable basis for identification.[26] Health care data that does not satisfy this definition may be collected, used, and disclosed by a company without running afoul of HIPAA. For example, where health information has been de-identified or aggregated without disclosing individual identifiers, it does not constitute PHI and may be disclosed without an individual's consent or authorization.[27] In State ex rel. Cincinnati Enquirer v. Daniels, for instance, the Ohio Supreme Court held that the Cincinnati Enquirer could obtain copies of lead-contamination notices issued by the Cincinnati Health Department.[28] The court found that the notices did not reveal PHI even though they referenced an unnamed child whose blood test showed an elevated lead level.[29] Similarly, guidance on HHS's website notes that merely reporting the average age of health plan members is not PHI because the aggregated data does not identify any individual plan member.[30]

These limitations in HIPAA's scope present large regulatory gaps when applied to the digital health sector (except in those situations where a digital health product is provided directly by a HIPAA covered entity or in a business partnership with a provider or insurer). Today, with minor exceptions, most digital health companies do not qualify as covered entities or business associates, and remain unregulated by HIPAA. Similarly, some of these organizations may collect sensitive health data that does not qualify as PHI. When either of these scenarios occurs, the digital health company is not subject to HIPAA's privacy and security regulations, and may operate with significantly less federal oversight. The regulatory scheme created by HIPAA focuses largely on which entity holds the data, and not on the nature or sensitivity of the information being collected. This, in turn, allows a significant portion of the digital health sector to avoid compliance with these crucial HIPAA privacy and security standards.

C. FDA, FTC, and Medical Device Regulation

In addition to HHS's oversight of HIPAA, the Food and Drug Administration assumes a key role in the regulation of medical devices, including Internet-connected medical technology. The FDA's role, however, is limited primarily to ensuring the safety and efficacy of certain classifications of devices, and not all mobile or digital technologies will trigger

---

26 Id. § 160.103.

27 Id. § 164.502(d).

28 844 N.E.2d 1181 (Ohio 2006).

29 Id. at 523; Cuyahoga Cty. Bd. of Health v. Lipson O'Shea Legal Group, 50 N.E.3d 499, 501 (Ohio 2016)

30 Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last updated Nov. 6, 2015).

FDA scrutiny.[31] Moreover, FDA regulations are not typically geared towards protecting patient privacy or security. While the FDA has released voluntary guidance "for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices," this guidance is not mandatory.[32] The FDA does not require cybersecurity testing for any device, and relies on the device manufacturer to perform any voluntary security testing.[33] Further, the FDA does not regulate device privacy, leaving such devices to be covered (if at all) by HIPAA.

Similarly, the Federal Trade Commission has played a crucial part in privacy policy, enforcement, and best practices since the 1970s.[34] The FTC is an independent federal agency responsible for protecting consumers and promoting competition. While the FTC is not specific to health care, its regulatory authority extends to unfair and deceptive acts or practices, which may occur in the health care industry.[35] In particular, the FTC can bring enforcement actions to halt violations of privacy and security laws. The FTC has brought more than 500 enforcement actions to protect consumer privacy, and these actions address a wide range of issues, including spyware, mobile devices, file sharing, and spam.[36] Cases may also involve non-adherence to a privacy policy. Similarly, the FTC has initiated over 60 cases since 2002 against companies that failed to adequately protect consumers' personal data.[37] In this manner, FTC's authority is broad, but is not directed at preventing or regulating privacy and security standards in the health care industry. Instead, FTC acts as a watchdog to enforce existing privacy and security standards, but does not create those standards. Thus, while FTC may enforce existing privacy and security laws in the digital health context, it does not address legislative gaps that may leave digital health technology unregulated.

---

31 See Kirk J. Nahra, *New York Attorney General Addresses Key Health Care Privacy Gaps*, WILEY REIN (Apr. 2017), https://www.wileyrein.com/newsroom-newsletters-item-April_2017_PIF-NY_AG_Addresses_Key_Health_Care_Privacy_Gaps.html (last visited Aug. 28, 2018, 03:15 PM).

32 Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, U.S. FOOD & DRUG ADMINISTRATION 4 (Dec. 28, 2016), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf (last visited Aug. 28, 2018, 01:43 PM).

33 Adam Brand, *Closing the Gap in Medical Device Cybersecurity*, PROTIVITI (Jan. 3, 2018), https://blog.protiviti.com/2018/01/03/closing-gap-medical-device-cybersecurity/ (last visited Aug. 28, 2018, 01:43 PM).

34 Protecting Consumer Privacy and Security, FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security (last visited Sept. 29, 2018, 04:33 PM).

35 See Privacy & Data Security Update:2017, FEDERAL TRADE COMMISSION, at 1 (Jan. 2017 – Dec. 2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf (last visited Sept. 29, 2018, 04:19 PM).

36 Id. at 1-2.

37 Id. at 4.

D. State Regulatory Frameworks

As the gaps associated with federal legislation become more apparent, states have begun stepping in to ensure comprehensive privacy and security standards apply to digital health. In March 2017, for example, New York Attorney General Eric Schneiderman announced that his office settled three cases with various mobile health applications for insufficient or inappropriate privacy practices, and misleading privacy and security claims.[38] In bringing these cases, New York acted to fill a regulatory gap in FDA oversight—these digital health devices had not triggered FDA review—and the HIPAA Privacy Rule.[39] Specifically, although digital health devices were being used in these cases, the companies did not qualify as covered entities and, therefore, no federal privacy structure governed these organizations. The New York Attorney General stepped in to ensure privacy protections would be applicable to these digital health applications despite the absence of a comprehensive federal regulatory structure.[40] Such action signifies a potential shift toward "regulation through enforcement,"[41] which states may begin to use more frequently if federal privacy and security standards are not properly updated.

In addition to New York's enforcement action, states have also begun implementing legislation to patch the holes in federal regulations. The most recent and innovative action by a state is S.B. 327, a cybersecurity bill governing Internet of Things devices in California.[42] California Governor Jerry Brown recently signed this bill into law, making it the first state in the nation to adopt IoT legislation. This new law, which becomes effective on January 1, 2020, will mandate that any manufacturer or developer of a "smart" device—including connected health devices—ensure that the product is equipped with reasonable security features to protect the device and the information it houses.[43] Advocates of the bill hope that the new law will focus nationwide attention on the issue of IoT security, which extends beyond state boundaries.

Legislation, such as S.B. 327, is intended to bridge gaps in federal regulatory frameworks. Whereas a digital health company may escape HIPAA's grasp because it does not qualify as a covered entity, the company would still be subject to minimum privacy and security standards if it conducts business in California. The goal of such legislation is to minimize opportunities for organizations to collect sensitive data without being subject to some form of regulatory structure simply because the pace of technological innovation outpaces policy discussions.

As the nation reacts to S.B. 327, it will be interesting to observe whether other states implement comparable legislation, and whether upcoming bills will spur the federal legislature to create a comprehensive regulatory framework. Addressing privacy and security for

---

38 Nahra, supra note 31.

39 Id.

40 Id.

41 Id.

42 Senate Bill No. 327 (Cal. Sept. 28, 2018), available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327 (last visited Sept. 29, 2018, 03:19 PM).

43 Id.

digital health and other Internet-connected devices on a state-by-state basis risks inconsistent standards and approaches, which could make it more difficult for digital health companies to determine their obligations, duties, and responsibilities. Comprehensive federal legislation could add consistency and predictability to privacy and security standards in digital health. However, until the federal legislature takes action, such standards will have to be developed and enforced by states and industry organizations.

V. THE DANGERS OF NON-REGULATION

Inconsistent or non-regulation of health care entities presents numerous risks that are unacceptable to both organizations and patients. Importantly, the lack of a mandatory regulatory regime may lead some digital health companies to avoid basic privacy and security practices altogether and endanger patient data. In many instances, economic incentives can cause digital health companies to push their devices to market with little consideration for security measures.[44] These devices, in turn, may be particularly susceptible to hacking, which can lead to the unauthorized acquisition of patient health data. Moreover, these devices may operate on larger health care networks and create backdoor entry points to accessing data from an entire health system that is otherwise secure. Such devices not only jeopardize the confidentiality and integrity of their own users' data, but also have the potential to create widespread breaches of health data at larger institutions.

Moreover, consumers are often not equipped to understand the difference between covered entities and non-covered entities and how this distinction drives digital health compliance. Instead, consumers may assume that their sensitive health data is protected and that adequate security measures will protect them from harm despite a contrary reality. The current regulatory framework assigns consumers the hardship of understanding the applicability of complex legal regulations to protect their own privacy and security.

Consumers, however, are not the only group harmed by gaps in digital health regulation. Digital health innovators and entrepreneurs are also adversely affected. In particular, having separate rules that apply to covered and non-covered entities can create confusion among tech innovators as to whether their products would be regulated under federal frameworks. This uncertainty may result in hesitant investors, which can delay or stifle technological innovation in the health care industry.[45] Further, a breach from lax security practices may cause immense reputational damage to the digital health company.

VI. ENCOURAGING COMPLIANCE

While federal regulatory compliance may not be mandatory for a large portion of the digital health industry, digital health companies should nonetheless ensure they are adhering to adequate privacy and security standards. The reason for this is, at a minimum, three-

44 See Paul Merrion, DHS Warns Insecure Internet of Things Could Spur Product Liability Lawsuits, CQ ROLL CALL WASH. DATA PRIVACY BRIEFING (Nov. 16, 2016), available at 2016 WL 6774799.

45 Alexis Guadarrama, *Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry*, 55 (4) HOUSTON LAW REVIEW 999, 1017 (2018).

fold. First, consumers expect minimum privacy and security standards to be associated with their products, and can negatively impact a company's market share if that company fails to satisfy consumer expectations. Second, it is inevitable that unregulated digital health companies will eventually be subject to a privacy and security regulatory scheme. While the form of this comprehensive regulatory framework is currently unknown, the risks associated with unregulated digital health products are too great to leave this industry unattended. This has become evident with California's implementation of S.B. 327—if the federal legislature does not act, states will. Companies that delay implementing basic privacy and security standards now will be adversely impacted if a new regulatory structure takes effect. Moreover, it is likely that regulations for digital health companies will mirror privacy and security best practices in effect today. Digital health companies have the opportunity now to build strong compliance programs and privacy policies, which will result in a smooth transition under future regulations.

Finally, by participating in the privacy and security dialogue today, digital health companies can help establish the standards and requirements for future regulations that will govern their industry. Public-private stakeholder participation is actively encouraged as policymakers think through how to regulate new technologies without stifling innovation.[46] By engaging with privacy and security concerns today, digital health companies can advocate for regulations that will promote their business interests while protecting consumer data.

The question then becomes which frameworks should digital health companies adhere to when implementing privacy and security standards? The obvious choice is HIPAA, particularly for data security, even though its requirements are not yet mandatory for a significant portion of the digital health industry. As an established framework governing health care privacy and security compliance, HIPAA contains sufficient flexibility to adapt to varied circumstances and organizations, including digital health. By voluntarily complying with HIPAA (or trying to meet its standards where they make sense for the business), digital health companies can ensure they are implementing best practice standards in effect for the health care industry. Such compliance will also create consistency across the health care sector and avoid inconsistent application of privacy and security rules. Consumers will be better able to gauge their privacy and security rights and remedies with uniform implementation of HIPAA's rules. Indeed, numerous experts have counseled in favor of expanding HIPAA's reach to the digital health industry.[47] The downside to voluntary compliance with HIPAA, however, is not only the costs associated with implementing adequate standards, but also the concern that the traditional TPO model of disclosure under HIPAA may not fit well with consumer facing products.

An alternative is for digital health companies to implement industry-created cybersecurity

---

46 See Bethany Corbin & Megan Brown, *Partnerships Can Enhance Security in Connected Health and Beyond*, CIRCLEID (Dec. 14, 2017, 8:30 AM), http://www.circleid.com/posts/20171213_partnerships_can_enhance_security_in_connected_health_and_beyond/ (last visited Sept. 30, 2018, 05:19 PM).

47 See Mary Butler, *Is HIPAA Outdated? While Coverage Gaps and Growing Breaches Raise Industry Concern, Others Argue HIPAA is Still Effective*, 88 J. AHIMA 14 (2017), http://bok.ahima.org/doc?oid=302073#.W6TW0a2ZP-Y (last visited Sept. 29, 2018, 03:19 PM).

frameworks. Many HIPAA-regulated entities also follow one or more security frameworks developed by industry professionals to enhance the security and availability of patient data. Numerous frameworks exist, enabling digital health companies to adopt the framework that best meets their organizational structure and needs. The 2018 HIMSS Report surveyed health care organizations and identified the five primary security frameworks in use throughout the health care industry today:[48] (1) National Institute of Standards and Technology (NIST);[49] (2) Health Information Trust Alliance (HITRUST);[50] (3) Center for Internet Security (CIS) Critical Security Controls;[51] (4) International Organization for Standardization (ISO);[52] and (5) Control Objectives for Information and Related Technologies (COBIT).[53] Adoption of one of these voluntary cybersecurity frameworks will assist digital health companies with remaining up-to-date on cybersecurity hygiene and can offer insight into guarding against common security threats affecting the industry

VII. CONCLUSION

Digital health represents an advantageous development to enhancing patient wellness and health care delivery in the United States. With the potential to lower medical costs and serve broader patient populations, digital health is only projected to grow in the coming years. As this technological frontier develops, it is crucial that federal regulations evolve to safeguard patient privacy and security. The current regulatory framework for the health care industry contains significant gaps that exclude a majority of digital health companies from necessary federal oversight in their data collection practices. As Congress considers the most effective method to remedy these gaps, digital health companies should be proactive in their approach to privacy and security, including voluntary compliance with HIPAA and industry-created cybersecurity frameworks. Such proactive behavior not only promotes consumer confidence in the digital health company, but also enables the company to contribute to the dialogue on best practice standards for the digital health industry.

---

48 HIMSS, *2018 Himss Cybersecurity Survey,* 18 (2018), https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Sept. 28, 2018, 02:49 PM).

49 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited Sept. 28, 2018, 03:19 AM).

50 CSF Version 9.1, HITRUST, https://hitrustalliance.net/hitrust-csf/ (last visited Sept. 21, 2018, 10:35 AM).

51 Download the CIS Controls V7 Today, CENTER FOR INTERNET SEC., https://learn.cisecurity.org/20-controls-download (last visited Sept. 21, 2018, 11:03 AM).

52 ISO 27001 - Information security management systems, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, https://www.iso.org/isoiec-27001-information-security.html (last visited Sept. 21, 2018, 10:42 AM).

53 COBIT 4.1: Framework for IT Governance and Control, ISACA, https://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx (last visited Sept. 21, 2018, 10:44 AM).

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

DIGITIZATION IN THE HEALTH SECTOR IN THE TRADE-OFF BETWEEN TECHNICAL AND LEGISLATIVE POSSIBILITIES AND LEGAL LIMITS ACCORDING TO GERMAN LAW[1]

Anna Kristina Kuhn & Marie-Isabel Heinz

AUTHORS

Anna Kristina Kuhn, LL.M. (Medical law) is a German lawyer specialized in medical law, advising health care professionals and other suppliers in the health sector for rehborn.rechtsanwälte in Dortmund since 2016. She represents her clients in and out of court in the entire field of medical law. Her focal areas of specialization are medical malpractice law, hospital law and physicians' professional law. She is currently working on her doctorate on a medical law topic and regularly publishes papers in the German journal Gesundheitsrecht (Health Law).

Marie-Isabel Heinz, LL.M. (Medical law) is a German lawyer specialized in medical law, advising pharmaceutical companies and other stakeholders in the health sector at Sträter Lawyers in Bonn since 2017. Her focal areas of specialization are the regulatory and contractual aspects of clinical trials of medicinal products and medical devices, data privacy and data protection aspects in the health care sector as well as questions of regulatory matters and national or European approval procedures.

ABSTRACT

In May 2018, the 121st German Medical Association in Erfurt decided to relax the prohibition of exclusive remote treatment which had previously been standardized in the Model Professional Code of Conduct for physicians working in Germany (MBO-Ä). With this, the German Medical Association has responded to the continuing call for progress and further development in terms of digitization. Nevertheless, many questions remain unanswered, such as the implementation and interpretation of the provisions of § 7 para. 4 MBO-Ä in its new wording and their embedding in existing regulations. Data protection, which defines the legal limits of remote treatment, also plays an important role here.

---

1 This paper will be published in parallel in German language under the title *Digitalisierung in der Medizin im Spannungsfeld zwischen technischen und legislativen Möglichkeiten und rechtlichen Grenzen* in GesR issue 11/2018.

TABLE OF CONTENTS

I. INTRODUCTION

Digitization in the health sector has been a perennial issue in legal and medical expert discussions for several years now. The respective legislative progress can be considered rather sluggish, not least because of the controversial picture of opinions. Despite the high number of supporters in favor of digitization in health care, the amount of critics and skeptics is decreasing slowly.

The supporters of remote treatment see an advantage for improving health care, especially regarding the demographic changes and the shortage of physicians, not only in rural areas. Moreover, due to the possibility of offering short-term consultations, improvements in quality of medical services are predicted. Not only the fully employed patient appreciates remote treatment as a huge timesaver. Besides, the risk of infection in the physician's office can be reduced. Critics of (exclusive) remote treatment fear that the trustful relation between patient and physician might suffer from the lack of personal contact. An increase of diagnostic errors is predicted due to a restriction in the possibilities of perception and cognition. Last but not least, the "new" digital methods of data transfer imply a higher risk for the highly sensitive patient health data[2].

The physicians' professional code in Germany reflected these concerns and the requirements for patient safety in its former version, valid until the decision of the 121st German Medical Association in May 2018. In contrast, neighboring countries such as Switzerland have already permitted exclusive remote treatment – without being swamped with reproaches of medical malpractice. Foreign providers of remote treatment have already established themselves on the German market by requisitioning German physicians[3]. This shows that a "head-in-the-sand-policy" can have counterproductive effects on digitization. The decision of the German Medical Association in May 2018 on opening the ban of exclusive remote treatment is therefore to be welcomed.

Needless to say that despite all the euphoria about digital progress and digital freedoms, the patient health data concerned, which are particularly sensitive in relation to fundamental rights, should not be neglected. However – and this aspect is often overlooked – data protection requirements are applicable not only for remote treatment, but also in every "conventional" physician's office. Regarding the possibility of fast transfer of large datasets and the resulting increased risk potential[4], data protection becomes more virulent

---

2 For advantages and disadvantages cf. Peter Kalb, *Rechtliche Aspekte der Telemedizin (Legal aspects of telemedicine)*, 8, GESR, 481, 483 (2018).

3 Cf. speech of the president of the German Medical Association and the German Physicians' Board, Prof. Dr. Frank Ulrich Montgomery, *Opening of the 121st German Physicians' Board in the Steigerwaldstadion Erfurt on the 8th of May 2018*, 9, https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/121.DAET/Eroeffnungsrede_Prof._Montgomery.pdf (last visited Sept. 28, 2018).

4 Already: Wilfried Berg, *Telemedizin und Datenschutz (Telemedicine and data protection)*, 8, MEDR, 411, 413 (2004) with further references.

in the context of telemedicine.

II. LEGAL POSSIBILITIES OF REMOTE TREATMENTS IN GERMANY

The revised version of § 7 para. 4 sentence 3 MBO-Ä now reads as follows: "Exclusive consultation or treatment via communication media is permitted in individual cases if this is medically justifiable and the necessary medical care is maintained, in particular through the way in which findings are made, consultation, treatment and documentation are provided, and the patient is also informed about the special features of exclusive consultation and treatment via communication media.". In the future, patients should be provided with medical care that corresponds to the recognized state of medical knowledge, which includes the further development of telemedicine, digital, diagnostic and other comparable possibilities, without establishing a model of primary telemedicinal treatment. The personal doctor-patient contact should thus continue to be regarded as the "gold standard" of medical treatment[5]. But what does the change of the MBO-Ä mean for physicians? How is the new regulation to be interpreted? And: How does it fit in with other legal systems in force?

A. Physicians' Professional Law

The reformulation of the MBO-Ä alone does not change anything for the attending physician. The MBO-Ä itself has no legal norm quality and therefore needs to be transposed into the professional regulations of the Federal States' Chambers of Physicians. Although the MBO-Ä is not legally binding, it nevertheless serves as a guidance for the Federal States' Chambers of Physicians, so that the earlier prohibition of exclusive remote treatment (old § 7 para. 4 MBO-Ä) has also been adopted analogously by all Federal States' Chambers of Physicians in their professional regulations. Today, however, this no longer applies without restrictions. In summer 2016, the State Chamber of Physicians in Baden-Württemberg has already changed its professional regulations and approved remote treatment of Baden-Württemberg patients by Baden-Württemberg physicians for model projects. This year, the Federal States' Chambers of Physicians of Schleswig-Holstein and Saxony have also legitimized the exclusive remote treatment in cases of medical justifiability by amending the respective Professional Code of Conduct.
Finally, the representatives' meeting of the Rhineland-Palatinate State Chamber of Physicians – very recently – decided on 20th September 2018 on a corresponding new regulation of the Professional Code of Conduct.

It can be assumed that other regional Chambers of Physicians will amend their professional regulations in accordance with the new provisions of § 7 para. 4 MBO-Ä. On the

5 *Synopsis of the changes in § 7 Abs. 4 MBO-Ä (remote treatment)*, https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/MBO/Synopse_MBO-AE_zu_AEnderungen____7_Abs._4.pdf (last visited Sept. 28, 2018).

other hand, in May 2018 the Saarland Chamber of Physicians – following the resolution of the 121st German Medical Association – expressly spoke out against a relaxation of the prohibition of exclusive remote treatment[6], with the result that the professional law will probably be fragmented in this respect. In the context of remote treatment, the question of the applicable professional law will therefore soon arise.

The physician is a compulsory member of the regional Chamber of Physicians in whose district he practices his profession. He is therefore also subject to their professional code of conduct. In the case of a "normal" visit to the doctor, it is clear that the doctor exercises his profession at the office. But does this also apply if the doctor offers online video consultation hours from his practice, during which he treats patients from other chamber districts? There is much to be said in favor of continuing to determine the physician's place of business as the place where he exercises his profession[7]. A different understanding would lead, in particular, to considerable practical difficulties. Based on the patient's actual whereabouts during treatment – which could alternatively be taken as a basis – the attending physician would possibly become a compulsory member of a large number of regional chambers of physicians, which in turn could lead to an unreasonable burden on the exercise of the physician's profession. Ultimately, determining the patient's actual whereabouts could also mean unreasonable additional work for the doctor. All this would in any case make remote treatment extremely unattractive from a medical point of view, so that the desired progress would not be achieved.

B. New wording of § 7 para. 4 of the Model Professional Code of Conduct (MBO-Ä)

According to § 7 para. 4 sentence 3 MBO-Ä in its new wording it should definitely be decisive in the future whether the attending physician considers the exclusive remote treatment to be medically justifiable in the individual case. But when is remote treatment medically justifiable? And what defines an individual case? There is no legal definition for this.
It is safe to assume that the previously permitted options of remote treatment will also be permitted under the new regulation[8]. However, the new regulation is expressly intended

---

6 Cf. Andeas Kindel, *Fernbehandlung, Saar-Ärzte fürchten Kontrollverlust (Remote treatment, Saar-physicians fear loss of control)*, ÄRZTEZEITUNG ONLINE (May 2 2018), https://www.aerztezeitung.de/politik_gesellschaft/berufspolitik/article/963095/fernbehandlung-saar-aerzte-fuerchten-kontrollverlust-telemedizin.html (last access Sept. 28, 2018).

7 The question of the professional law also arises in particular with regard to the cross-border telemedical activities of physicians who are established in another EU member state.

8 § 7 para. 4 MBO-Ä (old version) has not standardized a general prohibition of remote treatment measures, rather only diagnosis and therapy recommendation for unknown patients via print and communication media – i.e. in the context of the first contact – should be completely prohibited by this law, cf. in this regard: *Notes and explanations of the Federal Chamber of Physicians on § 7 para. 4 MBO-Ä (remote treatment)*, 11.12.2015 https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/2015-12-11_Hinweise_und_Erlaeuterungen_zur_Fernbehandlung.pdf (last visited Sept. 28, 2018); Anna Kristina

to permit other forms of remote treatment, in particular the initial contact via means of communication.

In order to determine the regulatory content, the view taken here is that the principle of freedom of medical treatment recognized by the highest court[9] and the case-law on medical liability can be relied upon. Medical freedom of therapy means here that the physician can in principle choose the examination and treatment methods – among the permissible treatment methods – freely, he thus possesses a discretionary and judgmental scope in this respect[10]. This means that the proper course of medical action is determined exclusively by whether the physician has made justifiable decisions about diagnostic and therapeutic measures using "the medical knowledge and experience required from him in the specific case and has carefully implemented these measures"[11].

Correctly, the physician must therefore ask in relation to the intended purpose what "form of depth of the physicians' perception of the patient is necessary for the physician for standard treatment"[12]. The physician must therefore assess the risks of remote treatment on his own responsibility on a case-by-case basis, i.e. in relation to the treatment and the patient. As soon as the doctor considers a personal visit of the patient to be indicated, he has to point this out to the patient and interrupt the remote treatment. As with any other therapy recommendation, it is then up to the patient to actually follow this up.

If the physician decides to carry out remote treatment, even though this was not medically justifiable in the individual case, this violation of professional duties can lead to civil liability.
The choice of a medically unjustifiable form of therapy can quickly be regarded as a gross medical malpractice in a lawsuit.

The physician should also pay special attention to patient information, because in the context of remote treatment the physician must also inform about the special features of consultation and treatment exclusively via communication media. The obligatory content of this information is not defined, but can also be determined according to the traditional principles. However, it is recommended to expressly point out to the patient that not all diagnostic possibilities, such as palpating, can be used in the context of remote treatment – even if this is likely to be self-explanatory to the patient on a regular basis. This recommendation applies at least as long as there is no highest court jurisdiction on

---

Kuhn, *Grenzen der Digitalisierung der Medizin de lege lata und de lege ferenda (Limits to digitization in health care de lege lata and de lege ferenda)*, 12, GESR, 748 (2016).

9 Cf. BGH (German Federal Supreme Court), decision dated Sept. 22, 1987 – VI ZR 238/86, NJW 1988, 763, 764.

10 LAUFS/KERN, HANDBUCH DES ARZTRECHTS (MANUAL OF MEDICAL LAW), § 97 Rn. 36, (4th ed. 2010).

11 BGH (German Federal Supreme Court), decision dated March 10, 1987 – VI ZR 88/86, NJW 1987, 2291, 2292.

12 Michael Hahn, *Telemedizin und Fernbehandlungsverbot – Eine Bestandsaufnahme zur aktuellen Entwicklung (Telemedicine and ban of remote treatment – an inventory of the latest developments)*, 36, MEDR, 384, 386 (2018).

this, because in a medical liability lawsuit the physician has to prove the correctness of the information. The special information and consent should also be included in the patient documentation.

C. Federal regulations

The amendment of the MBO-Ä or the professional law alone is not sufficient to reasonably integrate remote treatment into the system of medical care. Rather, an extensive action by the legislator is required here. Some statutory provisions currently stand in the way of an effective offer of remote treatment services – this is illustrated by the example of the provisions of § 9 of the German Act on Advertising of Medicinal Products (HWG) and § 48 of the German Medicinal Products Act (AMG).

1. § 9 German Act on Advertising of Medicinal Products (HWG)

According to § 9 HWG, advertising for the recognition or treatment of diseases, sufferings, bodily injuries or pathological complaints that are not based on the physician's own perception of the patient is not permitted. Although it is not the remote treatment itself that is prohibited, but only the advertising for the same, the provision under the law on therapeutic product advertising nevertheless stands in the way of an appropriate offer of remote treatment services. There is no distinction according to whether distance treatment is permissible or inadmissible under professional law, so that the wording of the provision is clear. It is well known that the wording represents the limit of any interpretation. Any interpretation to the effect that forms of remote treatment permitted under professional law are not covered by the advertising ban cannot be made for this and other reasons[13]. The medical professional codes of conduct are established as statutory law in the hierarchy of norms below formal statutory law. The result of an interpretation cannot be that the formal-legal prohibition norm of § 9 HWG is leveraged by sublegal statute right. In addition, this type of interpretation would (probably) lead to the fact that federal law would have to be interpreted inconsistently in the individual chamber districts, since - as previously described - not all regional medical associations have adopted or will adopt the opening clause adopted in the MBO-Ä in their professional regulations.

According to the opinion represented here, it is questionable whether the "mere" offering of remote treatment services on a doctor's homepage is already to be regarded as advertising in the sense of the provision[14]. However, this is possible in individual cases, depending

---

13 Different view: Julia Braun, *Die Zulässigkeit von ärztlichen Fernbehandlungsleistungen nach der Änderung des § 7 Abs. 4 MBO-Ä (The admissibility of remote treatment services after the change of § 7 para. 4 MBO-Ä)*, 36, MEDR, 563, 566 (2018); Michael Hahn, *Telemedizin und Fernbehandlungsverbot – Eine Bestandsaufnahme zur aktuellen Entwicklung (Telemedicine and ban of remote treatment – an inventory of the latest developments)*, 36, MEDR, 384, 386 (2018).

14 According to the Ministry for Social Affairs and Integration of the State of Baden-Württemberg, remote treatment in the context of public services should not be subject to the advertising concept of § 9 HWG, cf. LT B-

on the form it takes, due to the broad advertising concept of the law on the advertising of therapeutic products[15]. Enabling the provision of exclusive remote treatment services without mentioning this on the homepage, on the other hand, would be a waste of time. Even if the legal literature rightly raises the question of whether "own perception" within the meaning of § 9 HWG requires an offline contact purely conceptually[16], this will not lead to a legally secure solution for the physician. In any case, it has already been decided in the case law of higher courts that remote treatment within the meaning of § 9 HWG is to be present if the treating person makes a diagnosis or submits treatment proposals solely on the basis of written information, information provided by telephone, other media or third parties at a distance[17]. Undoubtedly, the online video consultation should also be subsumed under this heading. Legislative action is therefore absolutely necessary, not least because a violation of § 9 HWG under § 15 para. 1 No. 6 HWG constitutes an administrative offence, which can be punished with a fine of up to € 50,000.00 (§ 15 para. 3 HWG).

2. § 48 German Medicines Act (AMG)

Pursuant to § 48 para. 1 sentence 1 AMG, medicinal products intended for human use may not be supplied if there has obviously been no direct contact between the doctor and the person to whom the medicinal product is prescribed prior to medical treatment[18]. According to § 48 para. 1 sentence 3 AMG, exceptions may be made in justified exceptional cases, in particular if the patient and doctor know each other from a previous direct contact or if the treatment is merely repeated or continued. This provision therefore at least opens up the possibility of interpretation to the effect that in the case of remote treatment permitted under professional law, there is a justified exception within the meaning of the provision. However, this conclusion is by no means mandatory, so that § 48 AMG also precludes a meaningful offer of distance treatment services.

W printed matter 16/3161 p. 3. This interpretation is, however, at least questionable, since such restriction is not included in the wording of § 9 HWG.

15 Cf. on this topic: Julia Braun, *Die Zulässigkeit von ärztlichen Fernbehandlungsleistungen nach der Änderung des § 7 Abs. 4 MBO-Ä (The admissibility of remote treatment services after the change of § 7 para. 4 MBO-Ä)*, 36, MEDR, 563, 566 (2018).

16 Cf. Michael Hahn, *Telemedizin und Fernbehandlungsverbot – Eine Bestandsaufnahme zur aktuellen Entwicklung (Telemedicine and ban of remote treatment – an inventory of the latest developments)*, 36, MEDR, 384, 386 (2018).

17 OLG (Higher Regional Court) Munich, decision dated Aug. 2, 2012 – 29 U 1471/12, MMR 2012, 824.

18 On the concerns about this provision under European law see Ulrich M. Gassner, *Verbot von Online-Verschreibungen von Medikamenten: Patientenautonomie unter Dauerfeuer (Ban of online-prescriptions of medicines: patient autonomy under constant fire)*, LEGAL TRIBUNE ONLINE, March 31, 2016, https://www.lto.de/recht/hintergruende/h/arzneimittel-recht-online-rezept-kontakt-arzt-patient-gesetz-entwurf-bevormundung/ (last visited Sept. 28, 2018).

III. LEGAL LIMITS TO DIGITIZATION: DATA PROTECTION IN THE HEALTH SECTOR

The new provisions of data protection law must also be taken into account when assessing permissible remote treatment and its limits. Due to the "new" technical possibilities of the rapid exchange of large amounts of data, measures must be taken in the interest of the persons concerned and the principle of data economy to take account of this change. In this respect, the new regulations at least contribute to raising awareness, despite all the displeasure. What, then, must doctors pay particular attention to when offering remote treatment services relating to data protection?

A. GDPR and BDSG-new

The regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation, hereinafter referred to as "GDPR") entered into force on May24, 2016. In many places, however, it was only perceived shortly before or with its immediate commencement of application in all EU member states on May 25, 2018. It is intended to lead to a uniform application of the law and to give affected persons more control and transparency, especially in the digital age. The innovations go hand in hand with a tightening of the burden of proof on the part of those responsible for data processing. The GDPR addresses not only corporations such as Google, Facebook and Co., which were the primary target of the legislators in the reform, but also small companies, including physicians' offices, pharmacies and even privately run associations. The GDPR does not provide for the possibility of a general exemption for smaller units, but it does contain some exceptions, for example with regard to the requirement to appoint a data protection officer.

In addition to the introduction of the GDPR, which applies directly in all member states and does not require transposition into national law, the Federal Data Protection Act has also been amended in Germany and also entered into force on May 25, 2018 (BDSG-neu) by adapting some points to the European framework and filling in the reserved opening clauses. The criminal provisions are also reserved for the BDSG-new due to the lack of regulatory competence of the EU and can be found there in §§ 41 to 43 BDSG-new.

In terms of content, the principles of secure handling of personal data are not entirely new. Particularly with regard to sensitive data such as health data, the old BDSG, which implemented Directive 95/46/EC, already had high requirements. The increased requirements for information and proof obligations can therefore be implemented well by an appropriate internal data protection concept. Nevertheless, there are uncertainties in the interpretation of the Regulation with regard to individual special questions, which will be explained below and which will have to be answered in the near future by binding specifications of the European Data Protection Committee, the national data protection authorities and decisions of the courts.

B. Notions and definitions

First, the question arises as for which information the GDPR is applicable at all. According to Art. 4 No. 1 GDPR, personal data are "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more specific characteristics which express the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person". This includes in particular information such as first name and surname, address, telephone number, e-mail address and date of birth, which are collected as standard in the medical practice. This is referred to as simple personal data.

1. Health data

Particularly sensitive data such as health data are subject to special protection under the GDPR. Health data are defined in Art. 4 No. 15 GDPR as such "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status". According to recital 35 of the GDPR[19], this includes in particular information on past, present or future physical and mental health. The information is already personally identifiable if numbers, symbols or identifiers assigned to a natural person are used to uniquely identify that natural person for health purposes.
Examples of health data can therefore already be the insurance number, pre-existing conditions, diagnoses (indications), as well as all laboratory results, blood and tissue samples, but also disease risks attributable to a natural person.

2. Anonymization and pseudonymization

It should therefore be noted that - in accordance with recital 26 of the GDPR - pseudonymized data also clearly fall within the scope of the GDPR. This also applies if the person who receives and processes the pseudonymized data cannot draw conclusions about the natural person without consulting further information. Pseudonymization is defined in Art. 4 No. 5 GDPR as "the processing of personal data in such manner that it can no longer be attributed to a specific person without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". A classic example is the assignment of an identification number to a data set if the "allocation key" still exists.

19 The recitals are binding for the interpretation of the regulation.

Only for anonymous data the GDPR does not apply. However, the terms "anonymous" or "anonymization" are not defined. In general, anonymization is presumed when it is no longer possible to assign a person to a specific or identifiable natural person[20]. In this case, the allocation key for tracing the identification number back to the corresponding person must no longer exist.

The distinction between anonymization and pseudonymization plays an important role in the context of remote treatment, especially with regard to the transmission of data. In view of the new definition, the transfer of data to medical specialists can no longer be seen as anonymization, as it will always be possible to identify the person. In addition, the differentiation can become relevant when cooperating with pharmaceutical companies, e.g. when creating databases, registers or observational studies. Here, too, anonymization is only possible if neither the physician nor the pharmaceutical company can identify the individual patient.

It should also be emphasized that any operation relating to personal data constitutes processing within the meaning of Art. 4 No. 2 GDPR; even the collection, but also the mere deletion, is regarded as processing and no distinction is made between individual processing operations.

C. Legal bases for data processing

Furthermore, the fundamental prohibition of data processing without a legal basis, the so-called prohibition subject to permission, continues to apply. Corresponding legal bases can be found in Art. 6 para. 1 lit. a) to f) GDPR for "simple" personal data, in Art. 9 para. 2 lit. a) to j) GDPR for special categories of personal data, in particular health data, as well as in § 22 BDSG-new. Permission may be granted either by legal basis or by the express consent of the data subject.

Although consent is better suited as evidence, the use of a legal basis is likely to be more valuable overall - if a legal basis can be substantiated accordingly - as the consent can be revoked by the data subject at any time.

To determine the respective legal basis, each processing operation and the purpose of the data processing must be considered individually.

1. Medical treatment and health care as a legal basis

Generally, the collection of data by the physician should take place on the basis of the treatment contract and thus be permitted in accordance with Art. 9 para. 2 lit. h) GDPR in conjunction with § 22 para. 1 b) BDSG-new. A declaration of consent by the patient is

20 Cf. PAAL/PAULY/ERNST, DS-GVO KOMMENTAR (GDPR COMMENTARY), Art. 4 Rn. 49 (2nd ed. 2018).

therefore not usually necessary for "normal" treatment. However, due to the principle of purpose and data minimization (Art. 5 para. 1 lit. b) and c) GDPR), this only applies to the extent that data processing is necessary for the purpose, i.e. for carrying out the treatment, so that the scope of processing is limited to the extent necessary for this purpose[21].

But what is the necessary measure for a treatment via electronic communication media - e.g. the online video consultation? Is the assessment of necessity to be based on the performance of medical treatment in general, or on the specific form of treatment?

Referring to the treatment contract as a whole, it can be assumed that it is not necessary to use additional software to carry out the online video consultation, as the treatment contract can also be fulfilled in another way, namely by personal examination in the physician's office. The transmission of data by video goes beyond what is necessary, so that for the purposes of remote treatment a data protection consent would have to be obtained. Focusing, on the other hand, on the special form of treatment, i.e. remote treatment as such, one would come to the conclusion that no separate consent under data protection law has to be obtained, because the video consultation hour with the use of additional communication media is necessary to fulfil the treatment contract in its special form.

Also § 7 para. 4 MBO-Ä (new version) does not provide an answer to these questions, but only demands in medical regard that "the patient is also informed about the peculiarities of the exclusive consultation and treatment via communication media". An additional data protection clarification and informed consent is not expressly prescribed in any case - unlike, for example, § 40 para. 2a AMG for participation in the clinical trial.

In the direct contact between doctor and patient, the special type of data processing should be regarded as necessary according to the view held here. Finally the change of the MBO-Ä opens the clearance of the exclusive remote treatment for the physician in the context of its therapy choice and under consideration of the medical care to the physician. In the same way, within the framework of traditional treatment, he is free to decide on the manner and means of treatment in compliance with medical standards. Depending on which type of treatment he chooses, the appropriate implementation is necessary for the fulfilment of the specific treatment contract, so that no additional data protection consent is required in the context of remote treatment.

2. Informed consent for processing of patient health data

However, a direct transfer of personal health data, for example in order to obtain a (tele)consultation or in connection with a referral to a specialist - as in the context of conventional treatment - will only be possible with the consent of the patient, cf. also § 73

21 EHMANN/SELMAYR/HEBERLEIN, DSGVO KOMMENTAR (GDPR COMMENTARY), Art. 6 Rn. 5 (2nd ed. 2018).

para. 1b of the German Social Insurance Code (SGB V). It should be emphasized in this context that - as described above - pseudonymous data already fall within the scope of the GDPR. For this reason, the transmission of an X-ray image or ECG alone - without mentioning the patient's name - is already to be regarded as a processing operation[22]. The patient's consent must also be obtained for other purposes which go beyond the fulfilment of the treatment contract[23], e.g. the sending of appointment reminders. Since the transfer of data is often part of the treatment, the patient's general consent under data protection law will probably have to be obtained in these cases.

D. Further aspects of data protection

1. Rights of the data subject

It is important to note that, independent of the legal basis that permits the processing of personal data and health data, the data subject must always be informed in accordance with Art. 13 GDPR about the data collection in its concrete form - irrespective of whether the patient's consent under data protection law is obtained or not. Depending on the technical design, problems may arise with regard to the scope of the information obligations, for example if other players are involved in addition to the physician (e.g. platform operators). At a minimum, the physician must provide information on the identity of the person(s) responsible[24], the contact details of the data protection officer, the purposes of the processing, recipients or categories of recipients, the duration of the processing and the rights of the data subjects pursuant to Art. 15 et seq. GDPR to this effect. If the treatment is carried out exclusively via telephone/video telephony, the physician must also inform in this way. The reference to a notice in practice would therefore not be sufficient, but possibly data protection information on the doctor's website, if he actively refers to it during the online video consultation[25]. An exception to the duty to inform exists according to Art. 14 para. 5 lit. d) GDPR if the doctor has received the patient's data from a third party (permissibly) and they are subject to professional secrecy. This is the case, for example, if the primary care physician forwards the patient data to the specialist because it can then be assumed that the primary care doctor has already informed the patient comprehensively.

---

22 Different according to the former legal status; cf. Wilfried Berg, *Telemedizin und Datenschutz (Telemedicine and data protection)*, 8, MEDR, 411, 414 (2004).

23 Cf. on this topic: Joachim Schütz/Bernd Halbe, *Wann die Patienteneinwilligung notwendig ist (When patient consent is necessary)*, ÄRZTEZEITUNG ONLINE (MEDICAL JOURNAL ONLINE), Aug. 24 2018, https://www.aerztezeitung.de/praxis_wirtschaft/w_specials/datenschutzverordnung/article/969712/daten-verarbeitung-wann-patienten-einwilligung-notwendig.html (last visited Sept. 28, 2018).

24 For joint controlling see below under 4.b.

25 Also: recommendation of the North Rhine Chamber of Physicians, *Die DSGVO in den Praxisalltag integrieren (Integrating GDPR into the physician's routine)*, RHEINISCHES ÄRZTEBLATT (RHENISH MEDICAL JOURNAL), 8, 12 et seq (2018).

In addition, the requirements of Art. 9 para. 3 GDPR must be fulfilled. Accordingly, processing is only permissible if it is carried out "by specialist personnel or under their responsibility" and if this specialist personnel or the person responsible for data processing is subject to a statutory professional secret or other confidentiality obligation[26]. This shall include appropriate measures to safeguard the interests of the data subject and data security in general[27].

Furthermore, it must be ensured that the data subject can exercise his or her right to information (Art. 15 GDPR) and, if applicable, data portability (Art. 20 GDPR) without any problems. The latter means that the patient can request a copy of his patient file. However, it only exists if the processing is based on consent or a contract and is carried out using automated procedures. In the case of remote treatment, this means that the patient has no right to data transferability if the data processing is based - as described above - on the treatment contract as legal basis, since the legal basis of the health care and the treatment contract from Art. 9 para. 2 lit. h) GDPR is not mentioned in the concluding enumeration[28] of Art. 20 para. 1 a) GDPR[29]. The right of the patient to inspect the patient file according to § 630g of the German Civil Code (BGB) remains unaffected by this. In contrast to the right under Art. 20 GDPR, the physician is not given a deadline to react and the patient must bear the costs incurred himself.

Even if a third party is involved as platform operator, this should not lead to a different result: A contract within the meaning of Art. 6 para. 1 lit. b) GDPR would – if at all – be concluded between platform operator and physician - but not between platform operator and patient[30]. Apart from hat, however, only the processing of "simple" personal data by the platform operator would be permitted, which would not be sufficient for the desired purposes.

2. Joint controlling/Commissioned data processing

Since the GDPR came into force, there have also been new responsibilities for the involvement of several actors in connection with data processing. Art. 4 No. 7 GDPR defines the

---

26 Cf.EHMANN/SELMAYR/SCHIFF, DSGVO KOMMENTAR (GDPR COMMENTARY), Art. 9 Rn. 61 (2nd ed. 2018).

27 So called technical and organizational measures (TOMs) such as access restrictions, password protection, encryption and ensuring the integrity and availability of systems, etc., cf. Art. 24 para. 1 GDPR, § 22 para. 2 BDSG-new.

28 Cf. recital 68; PAAL/PAULY/PAAL, DS-GVO KOMMENTAR (GDPR COMMENTARY), Art. 20 Rn. 18 (2nd ed. 2018).

29 In the result also: Andreas Wolf, *Die Fernbehandlung nach dem 121. Deutschen Ärztetag im Lichte der DSGVO (Remote treatment after the 121st German Medical Association in the light of the GDPR),* 4, GUP, 129 et seq (2018).

30 Different view: Andreas Wolf, *Die Fernbehandlung nach dem 121. Deutschen Ärztetag im Lichte der DSGVO (Remote treatment after the 121st German Medical Association in the light of the GDPR),* 4, GUP, 129 et seq (2018).

person responsible as the person who alone or jointly with others differentiates between the purposes and means of data processing. Accordingly, anyone who collects, stores, transmits, etc. data for himself is responsible. Responsible person in the sense of the GDPR[31]. In contrast, the processor is, according to Art. 4 No. 8 GDPR, a person or body who processes personal data on behalf of the data controller. The delimitation is important because the responsible person and the processor have different obligations[32] and a corresponding agreement must be reached on the distribution of responsibilities in accordance with Art. 26 or Art. 28 GDPR.

Due to the contractual and professional duties of a physician to document patient data and to archive it beyond the treatment[33], the physician defines the processing purposes at least to this effect and is therefore generally to be regarded as the person responsible. The specialist to whom the referral is made by the family doctor also does not act as processor on behalf of the primary physician[34], since an independent legal relationship is established with the patient and he does not act on his behalf[35]. Cooperation between physicians and pharmaceutical companies - not only within the framework of clinical trials[36] - will also regularly be a joint responsibility, since in some areas decisions are made on data processing and corresponding internal regulations are required.

In the context of remote treatment, it is conceivable, depending on the technical implementation, that the physician may use one or more service providers who, in accordance with their dependence on the physician's mandate or their own influence on data processing, are to be classified as contract processors or joint responsible parties.

3. Data protection officer

In addition, the appointment of a data protection officer pursuant to Art. 37 GDPR will be necessary in practices offering remote treatment. Although the core activity of a medical practice mentioned in Art. 37 para. 1 lit. c) GDPR is not usually seen as an extensive

---

31 PAAL/PAULY/ERNST, DS-GVO KOMMENTAR (GDPR COMMENTARY), Art. 4 Rn. 55 (2nd ed. 2018).

32 At the same time, the obligations of commissioned data processors have increased and an independent liability has been established.

33 Cf. § 630 f para. 3 BGB, § 28 RöV (X-Ray Regulation).

34 According to the statement of the Data Protection Officer of North-Rhine Westphalia, which is no longer available, cf. *the resolution of the Concerted Action of the Professional Associations at the German National Association of Statutory Health Insurance Physicians*, June 22, 2018, http://www.kbv.de/html/35530.php (last visited Sept. 28, 2018).

35 Already: BGH (Federal Supreme Court), decision dated Jan. 14, 2010 – III ZR 188/09, NJW 2010, 1200; BGH, decision dated Jan. 14, 2010 – III ZR 173/09, NJW 2010, 1203.

36 Cf. *Short paper of the Data Protection Conference on Joint controlling*, March 19, 2018, https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/KP_16_GemeinsameVerantwortliche.pdf (last visited Sept. 29, 2018).

processing of personal data[37], it is subject to the duty to assess the impact of data protection due to the "use of new technologies" pursuant to § 38 para. 1 sentence 2 BDSG-new in conjunction with Art. 37 para. 1 GDPR, so that even smaller practices with less than ten employees must appoint a data protection officer when offering remote treatment. In addition, a list of processing activities in accordance with Art. 30 GDPR must be maintained in which the steps to be taken in connection with remote treatment must be listed as individual processing steps.

Finally, what are the consequences of the GDPR for breaches of data protection provisions? On the one hand, the framework for the imposition of fines has been drastically increased and can now amount to up to EUR 20 million or 4% of the annual turnover in the case of serious infringements, for example of consent requirements or the rights of the data subject pursuant to Art. 83 para. 5 GDPR. On the other hand, pursuant to Art. 82 para. 1 GDPR, the data subject has a claim for damages against the data controller and the processor if he or she succeeds in proving material or immaterial damage resulting from a breach of data protection.

IV. CONCLUSION

The amendment to § 7 para. 4 MBO-Ä (new version) is a first important step towards enabling exclusive remote treatment, which is becoming increasingly important in the course of digitization. Fortunately, it has now been recognized that the current attempt to close off the German healthcare market from remote treatment cannot be the future. The restraint of the medical profession in this regard can only be countered, however, if more legal clarity is created regarding the interpretation of the new professional regulations and regarding the possible consequences of the impending fragmentation of professional law with regard to the prohibition of remote treatment. In addition, legislative action is absolutely necessary, as the currently applicable statutory provisions blatantly stand in the way of a meaningful offer of distance treatment services. In addition to the professional limits, the physician in charge must also take into account the new data protection regulations, which will entail a number of organizational hurdles. Against the background of stricter accountability obligations and monetary liability risks, compliance plays an increasingly important role in this context.

37 Different view: Chamber of Physicians of the State of Hesse, which advises to appoint a data protection officer in health care institutions with less than ten employees at least for a transitional period of two years, cf. *Handout on Appointment of DPO in the view of the Chamber of Physicians of the State of Hesse*, https://www.laekh.de/images/Aerzte/Neues_Datenschutzrecht/Bestellung_eines_Datenschutzbeauftragten.pdf (last visited Sept. 29, 2018).

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

DATA POWER TO THE PATIENTS! PATIENT-DRIVEN DATA BUSINESS, NOT DATA-DRIVEN PATIENT BUSINESS

The Centrality of the Patient in the Commerce of Digital Healthcare [1]

Stefan Heinemann

AUTHOR

Prof. Dr. Stefan Heinemann works on ethical and business perspectives on digital Medicine and Artificial Intelligence. He is a studied philosopher and theologian, a professor of Business Ethics at the FOM University of Applied Sciences, Spokesman of the Ethics Ellipse Smart Hospital of the University Medicine Essen, member of the multi-stakeholder forum European AI Alliance and the Algorithm Monitoring Group of the Initiative d21, a long-time Vicerector of FOM University for applied Sciences in Germany (2011–2018), heads the Ethics of digital Healthcare & Medical research group at ifgs Institute for Health & Social Affairs and as an advisory board member in various research and educational institutions. Prof. Dr. Heinemann is, among others, a member of the Strategic Advisory Council of the BDA / BDI Federal Initiative "Creating a STEM Future", the Board of the Cologne Scientific Committee and Chairman of the "Science City Essen", and a member of the Board of Trustees of sneep – a student network for business and corporate ethics. In addition, he is the Chairman of the Scientific Advisory Board of Future Institute for Health Economics.

Twitter: @s_heinemann001
https://www.linkedin.com/in/prof-dr-stefan-heinemann/

ABSTRACT

Data-driven business models make up the medical and healthcare market in large parts, a trend reinforced by further technological developments and regulation. Care must be taken to avoid a situation where only a few players benefit. It's weird the patient has to become a customer in order to be a human being in the health business: The consistent empowerment of patients to handle their own data is essential.

---

1 Most parts of this article have already been published in HealthManagement.org 2018, Volume 18, Issue 6, p. 464-468. Some remarks and references were added.

TABLE OF CONTENTS

I. THE DIGITAL DATA WORLD IS BECOMING THE CORE OF MEDICINE AND HEALTHCARE

Who lives outside the GAMFANNAT economy (Google[2], Apple[3], Microsoft[4], Facebook[5], Amazon[6], Netflix[7], Alibaba[8], Tencent[9])? An increasing market capitalization of approximately $5 trillion (July 2018) – a multiple of the market value of all German DAX 30 companies together – and an even deeper connection of services and products with our increasingly digitally organized and experienced life clearly show that large parts of the global consumer society today and even more tomorrow and the day after tomorrow will become data-driven spheres. It is easy to imagine a world without fossil fuel-powered automobiles – but with flying autonomous vehicles, a bit harder without cell phones - and with brain implants - but a world without data in the sense of their intensive generation and usage, and practically in all areas of life – it seems to be hardly tangible (unless as a conscious and fairly complete renunciation of technology).

The development of data-driven activities as a whole is increasingly ethically questioned. In Germany, the Data Ethics Commission[10] has recently been created within the Federal Ministry of Interior, Building and Community, and in England the Data Ethics Framework[11] of the Department for Digital, Culture, Media and Sport. Today, it is equally un-

---

2 For insights into strategies and business cases for listed companies, investor relation platforms are helpful (alongside with (good) capital market research); Alphabet Investor Relations, https://abc.xyz/investor/ (last visited Oct. 20, 2018, 09:21 AM).

3 Apple Investor Relations, https://investor.apple.com/investor-relations/default.aspx (last visited Oct. 20, 2018, 09:11 AM).

4 Microsoft Investor Relations, https://www.microsoft.com/en-us/investor (last visited Oct. 20, 2018, 09:10 AM).

5 Facebook Investor Relations, https://investor.fb.com/home/default.aspx (last visited Oct. 20, 2018, 09:04 AM).

6 Amazon Investor Relations, https://ir.aboutamazon.com/ (last visited Oct. 20, 2018, 09:16 AM).

7 Netflix Investors, https://ir.netflix.com/ir-overview/profile/default.aspx (last visited Oct. 20, 2018, 09:23 AM).

8 Alibaba Group, https://www.alibabagroup.com/en/ir/home (last visited Oct. 20, 2018, 09:25 AM).

9 Tencent Corporate Governance, http://www.tencent.com/en-us/investor.html (last visited Oct. 20, 2018, 09:31 AM).

10 Datenethikkommission, Bundesministerium des Innern, für Bau und Heimat (Data Ethics Commission, Federal Ministry of the Interior, for Building and Community) https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/datenethikkommission/datenethikkommission-node.html (last visited Oct. 20, 2018, 09:37 AM).

11 *Guidance – Data Ethics Framework*, Department for Digital, Culture, Media & Sport (updated Aug. 30, 2018), https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework (last visited Oct. 20, 2018, 09:42 AM).

imaginable not using the digital advances in medicine – which are certainly critical in ethical terms, yet impressive, especially the data-driven ones – for positive precaution, diagnosis, healing and aftercare opportunities for patients and healthy people. From AI in radiology to precision medicine in oncology, people want to be, become, and stay healthy. Here a peculiar tension erupts.

In the GAMFANNAT world, considerably more people are using the services offered than would be expected in view of the level of trust that users have in their data usage – apart from the fact that hardly anyone, for example, really works through, understands or can decipher privacy statements. Transparency as a condition of the opportunity for fair consent looks different. To put it clearly: The GAMFANNAT Grandpa should not be sitting next to Lehman Granny. Nor is it to be expected that, in the end, patients will not give priority to the medical benefit of their data because of concerns about a "patient credit bureau" – even if the treatment contexts are hardly accessible to the individual patient. Convenience has always limited data protection requirements in real terms, and data protection should not be a luxury for the healthy. In addition, the GAMFANNAT players are already today – recognizable openly or only in contours – increasingly active in the medical and healthcare market and game changers.[12]

So what data-related opportunities and risks arise for patients from a business perspective? How can patients not only be masters of their data, but use data business cases for themselves? What is the value of their medical and health-related data? Which commercial, social or individual medical use of personal data makes sense and is as safe as it can be safe in the digital realm?

II. ECONOMICALLY, DATA IS NEITHER OIL NOR CURRENCY – BUT NEVERTHELESS THE CENTRAL FUTURE EXCHANGE UNIT FOR PATIENTS

Economically, oil is private property with exclusive ownership. My oil is my oil and only I can use it, nobody else. And when it's used up, it's gone. And I can only use one liter of

12 Google: Recently expansion into healthcare, strong strategic focus (*Google in Health*, GOOGLE https://www.google.com/intl/en_us/health/about/ (last visited Oct. 20, 2018, 10:01 AM)); Apple: Recently Apple Watch 4 has been classified as an FDA class 2 medical device and launched the project of medical clinics for employees, strong strategic focus (*Healthcare- The future of healthcare is in your hands*, APPLE, https://www.apple.com/healthcare/ (last visited Oct. 20, 2018, 10:12 AM)); Microsoft: Recently more azure services for next gen medical data (e.g. Genomics), strong strategic focus (*Health - Learn more about what Microsoft is doing in Health*, MICROSOFT, https://www.microsoft.com/en-us/enterprise/health (last visited Oct. 20, 2018); Facebook: Recently data sharing agreement with hospitals, growing strategic focus (Christina Farr, *Facebook sent a doctor on a secret mission to ask hospitals to share patient data*, CNBC (Apr. 5, 2018) https://www.cnbc.com/2018/04/05/facebook-building-8-explored-data-sharing-agreement-with-hospitals.html (last visited Oct. 20, 2018, 10:17 AM)); Amazon: Recently partnering with JPMorgan Chase and Berkshire Hathaway, yet unclear goal, probably using the sales and payment power of Amazon for healthcare, pharmacy or insurance to increase efficiency in healthcare (Zachary Tracer, *Amazon-Berkshire-JPMorgan Health Venture Takes Aim at Middlemen*, BLOOMBERG (Jun. 24, 2018) https://www.bloomberg.com/news/articles/2018-06-24/amazon-berkshire-jpmorgan-health-venture-takes-aim-at-middlemen (last visited Oct. 20, 2018, 10:22 AM)); also Netflix, Alibaba, Tencent are active, also Uber et al.

oil to the extent of one liter of oil. If I mix 1,000 liters of oil, it won't become "super oil". In economic terms, data have a completely different nature. I can share my data with multiple users, so they are not rivals, and when many different pieces of data come together, they create network effects that can in part lead to significant benefit increases. In addition, data can be copied virtually unlimitedly, does not wear out, can be transferred, and can be handled through access, use, and change, and distinguished into private club goods or public data assets (e.g. weather data). And you can do amazing mathematics with it: statistics is the new basic subject for understanding the data economy.

My personalized medical data may only have limited economic value for me – which may be existential – but economically cannot be increased arbitrarily. However, for a company, various data such as my personalized but also impersonalized data (anonymized, pseudonymized, or purely machine-generated) can, when aggregated, lead to completely new insights and offers, and in the end even to innovative value added – especially in modern data medicine, such effects are currently on the agenda, and therefore, for example, for the pharmaceutical industry, of great interest.

The emancipation of correlation versus causality does not take place in strict scientific theory, but in the pragmatic world of business models[13] – even with seriously anonymized data, cross-referencing and correspondingly smart data analysis models can often at least compensate for the information about the person that has been legally deleted, provided that those data are cleverly combined with other data (e.g. data from search engines or fitness devices) apart from that it is known that 87 percent of the US population can be re-identified by the combination of zip code, gender and date of birth.[14] Precisely because my data does not generally represent a significant value for me, there was – and is – a tendency to pass it quite relaxed to the companies in exchange for services and products. That's just how it is as a consumer: "If you are not paying for it, you're not the customer; you're the product being sold".[15]

In the end, to a large extent, the enormous market value of the corresponding data-driven companies is explained. Because they do not really share the cake. With a view to patients, this trend slowly begins to gain contours in the medical and healthcare sector. Strictly speaking, the medical data of patients is not a currency for patients themselves, because they are not a constant reference value, but depend essentially on their context. However,

---

13 To be very clear here: „In today's world, there is a growing tendency to trust personal beliefs, superstitions, and pseudoscience more than scientific evidence.", Helena Matute, Fernando Blanco, Ion Yarritu, Marcos Diaz-Lago, Miguel A. Vadillo & Itxaso Barberia, *Illusions of Causality: How They Bias Our Everyday Thinking and How They Could be Reduced*, 6 FRONTIERS IN PSYCHOLOGY, 888 (2015) – That is an unacceptable tendency. We should not let Bias become acceptable. It might be true, that rich people have big feet – if I hit the jackpot my feet will not grow - but that does not excuse to hit the other extreme: Of course correlation-based business models can make sense and produce value for customers.

14 Latanya Sweeney, *k-anonymity: a model for protecting privacy*, 10(5) INTERNATIONAL JOURNAL ON UNCERTAINTY, FUZZINESS AND KNOWLEDGE-BASED SYSTEMS, 557-570 (2002).

15 Andrew Lewis via Twitter, Sept. 13, 2010, available at: https://twitter.com/andlewis?lang=en (last visited Aug. 10, 2018, 03:25 PM).

data can replace financial transactions via their specific value – and yet, no oil, no currency, but an economic value that should be repaid.

III. BUSINESS MODELS FOR THE USE OF MEDICAL DATA AND IDEAS FOR DETERMINING THE VALUE OF DATA ARE DIVERSE AND RARELY RECOGNIZABLE TODAY

Which business models in the medical and healthcare industry use data and how is this money earned? This very simple-sounding question says it all. In principle, data can be traded or used directly (or as in the case of open-data provided without consideration, or data sharing). The GAMFANNAT economy usually does the latter and thus comes to steadily richer and deeper user experiences and increased, individual benefit, leading to a corresponding willingness to pay and, above all, loyalty – and last but not least, to competitive advantages. The algorithms of the companies are ultimately unregulated and in large parts even for an insider a black box – which makes the exact analysis of the value-added context not easier, as well as a social assessment (think of the potential for discrimination, currently the Berlin initiative d21[16] is taking corresponding first steps with the expert group "Algorithms Monitoring"). What is still emerging in medicine as personalized medicine, for example, is for consumers of media an everyday experience (certainly media are far less complex and consequential). Today we see no “MediFy”, but Spotify [17]

When it comes to trading data (as practiced by IQVIA[18], for example), transparency is less visible. Who really knows how their health insurance provider does the ultimately decisive risk assessment? Which data were used? The fact that you can no longer digitally live without advertising and this advertising is personalized on a data-driven basis, may cost some nerves and evoke countermeasures, such as paying for less advertising; others enjoy hyper-personalized content – but ultimately, it's a comparatively less critical data usage. With Patient Data Selling you will want to look more closely – and have to. The opt-out must always be possible for the patient, but today it is not. Just say “No” if you do not want to be part of the game (as long as it is doable for the average person). And a solution such as privacy-enhancing tools, which are available for online offers, for example, are far from available for medical data and records. The data system of the medical and health industry has a breathtaking opacity.

Good providers of data services will ensure transparency and participation, and legally

---

16 See: Netzwerk für die Digitale Gesellschaft (Network for the Digital Society), D21 https://initiatived21.de/ (last visited Oct. 20, 2018, 01:01 PM).

17 Spotify is partnering with DTC-Company Ancestry to combine playlists with DNA (*If you could listen to your DNA, what would it sound like?*, ANCESTRY, https://www.ancestry.com/cs/spotify (last visited Oct. 20, 2018, 01:15 PM) – sounds wired but entertainment is a valid way to create awareness and to start the empowerment, just think of gamefication as a means to create smart learning effects.

18 IQVIA, https://www.iqvia.com/ (last visited Oct. 20, 2018, 01:19 PM), founded 1982 (!) as Quintiles IMS Holdings.

offered to patients integrating them economically (and of course the doctors, who will soon be seeing new business models in the house, new risks but also new opportunities; no AI will ever replace a good heart (until we do not see an AI as an Existence in the full ethical sense) and doctors are always the natural intelligence needed, think of the actual critical discussion of Watson[19] (IBM)). And pay attention to the data quality: Statistical modeling is only suitable for intervention in medicine, if it has at least objectivity, reliability and validity with regard to the actual data used and the corresponding analysis methods. With good data, medical systems can be trained and multiple variables can cleverly be linked to newly empirically demonstrable correlations, which in turn may suggest prevention or therapy. Unfortunately, even with data success, neither the corresponding model can be verified nor a causality be proven. Statistics make more or less meaningful predictions depending on the sample size. But that's just what makes new hypotheses possible. And with the exponentially growing flood of information in the medical sector, it's difficult to avoid big data and AI (& Co.). In this sense, in my opinion, patients in the medical and healthcare sector want to deal with their data more sensitively than in previously common consumer areas – and hopefully do it well-informed – and in the end want to use the statistically usable or even personal data generated value.

On the other hand, what speaks in principal against patients paying in a transparent and well-structured manner, for example, special medical services in a smart hospital with their data? Self-pay may also be achievable for less wealthy patients. What speaks against a patient selling or licensing their genetic data for legal and legitimate and transparent purposes? In the upcoming DNA marketplace, the DNA "donors" should get an economic participation and become "business partners"; smaller companies such as EncrypGen[20] or Nebula Genomics[21] look for appropriate solutions, and often-key technologies such as Blockchain play a crucial role. Consequently, questions about the taxation of data will also have to play a bigger role in the future. And, of course, security and economic value issues – hacker attacks from outside and criminal energy within medical institutions – are likely to increase as the incentive potentially increases.

Patients may not have a clear understanding of what their data is really worth, and most of them might not care about the business models at this stage without recognizable participation (in a democratic sense). Companies in the medical and healthcare industry have a decisive advantage here, not least because the value of data constantly changes with the context of (today often unclear, but tomorrow...) business models. Of course, companies are often denied the final clarity on digital business models in the smart healthcare world. In the end, it will be crucial whether patients are adequately involved in certainly-not-

19 Annie Palmer, *IBM's Watson AI suggested 'often inaccurate' and 'unsafe' treatment recommendations for cancer patients, internal documents show*, DAILY MAIL ONLINE, https://www.dailymail.co.uk/sciencetech/article-6001141/IBMs-Watson-suggested-inaccurate-unsafe-treatment-recommendations-cancer-patients.html (last visited Oct. 20, 2018, 01:28 PM).

20 EncrypGen, https://encrypgen.com/ (last visited Oct. 20, 2018, 01:33 PM).

21 Nebula – Genomics, https://www.nebula.org/ (last visited Oct. 20, 2018, 01:34 PM).

marginal welfare gains. Enlightenment is likely to be necessary not only in legal but also in economic terms, otherwise consent declarations remain notoriously ineffective and economically not necessarily positive for the client or patient, because the data-collecting company determines what data it collects for what. But alternatives are also discussed, for instance, personal information management systems (PIMS[22]). Also important are Smart Communities to engage Patients in Dialogues about their data commercialization enterprise among themselves and with medical and other experts.

Not least so that the patients not only – as usual in the data economy from the customer's point of view – look for short-term benefits such as discounts or the like, but also take long-term positive effects into focus. This decision-making need not necessarily leads to the decision between added value and the protection of data but can combine both elements. It will not necessarily be about life-changing business when patients use their data or parts of their data economically. But then they are in the game, sitting at the table, and they also should sit there, if, in the end, it comes not through advertising but e.g. via insurance model-funded data platforms. At the end of the day, the patients themselves can increase the price and promote transparency by treating their data with the utmost care, which will be essential for an adequate position of providers (patients) towards buyers (companies). And today it is not foreseeable whether there will be minimal value added, exchangeable, or even a greater value added in the individual economic exploitation of individual, personalized or impersonalized data. A third way to do this would be to point out the current, ultimately unquestioning availability of data and self-marketing of the individual, which is likely to lead to lower prices through asymmetry.

Unlike other consumer data, medical data is absolutely necessary for factual medical care, but for the healthy some medical data are theoretically economically usable even without specific treatment, and not even prevention. Finally, the entire life as a prevention and data event is newly articulated in the quantified self. It will probably result in a holistic path connecting EMR Data, wearables, and B2C-driven genetic data. A conceivable impact can be the connection between pay and data exploitation, as it is known and practiced in the media industry[23]. The licensing of intangible assets answers the question as to which data, where, when, for how long, to whom and for what purpose and consideration are put into use.[24] Companies like to talk about "data ecosystems" as Terminus Technicus instead of "trade". Platforms to value and trade/licence C2B and maybe even C2C could

22 *Personal Information Management System*, European Data Protection Supervisor, https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en (last visited Oct. 20, 2018, 01:37 PM).

23 It is expectable that disruptive media businesses – e.g. in video gaming, music, film (content) and advertising (which see a digitalization-driven convergence tendency in their own value chains) – will cooperate with health data businesses (see footnote 6 for a recent example). One reason besides value creation might be located in the inner logic of these data-business.

24 Wolfgang Kerber, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection*, 11 (11) JOURNAL OF INTELLECTUAL PROPERTY LAW & PRACTICE, 856–866 (2016).

be an instrument – but always and only if Patients are educated to handle their medical data, which is for example for sure one of the challenges von DTC (direct to consumer) genomic businesses (23andme[25] etc.) because People are confronted with information (might it not be a diagnosis) which they maybe are not able to handle on their own without further professional advice, e.g. by a doctor.
In practice, such basically legal issues are not really resolved. In the case of personal data, the term "property" – or at least property-like entitlements – may be used, and in the case of non-personal data, it may be called a copyright aspect. Since there are many mergers of data forms that are likely to increase in the Internet of Things era, even this distinction with property reference may be difficult in practice, and thus the likelihood of lower transaction costs for personal data and its markets. The lawyers will get a lot to do.

If it is ethically correct and therefore legally required in a constitutional state to focus on the patient's benefit, and also economically attractive – albeit a little weird that the patient has to become a customer in order to be a human being with dignity in the health business – then the consistent empowerment[26] of patients to handle their own data is essential. And this does not in the least include the benefit that these can provide – only for the individual patient medically, but also financially, or, for example, by means of data donation in research, potentially for society as a whole or in cooperative models (eg Healthbank[27] in Switzerland). For this, a social consensus must be worked out that supports this form of economic participation. In addition, the lack of factual interoperability of existing patient records is a major obstacle for convincing implementation – and a significant costly one as well. There are initiatives such as MyData[28] from Finland, which generally demand a "human-centered personal data management" for data, and with the concept of the "Self-Sovereign Identity Systems" the final idea of the autonomy of users finds its way into the debate. New companies like Longenesis[29] also build on similar approaches.

25 23andMe, https://www.23andme.com/en-int/ (last visited Oct. 20, 2018, 01:56 PM).

26 Approaches such as gamification might be useful here, just as the inclusion of relevant multipliers in the educational realm, e.g. schools for continuing non-credit education (so-called „Volkshochschulen“ in Germany). In my opinion the issue of health data has to be addressed from kindergarten to higher education and for every target group – think of STEM Initiatives to foster tec talents for example.

27 Health Bank, https://www.healthbank.coop/ (last visited Oct. 20, 2018, 02:52 PM).

28 Mydata Finland, https://mydata.org/finland/ (last visited Oct. 20, 2018, 02:21 PM).

29 Longenesis, http://longenesis.com/ (last visited Oct. 20, 2018, 02:16 PM).

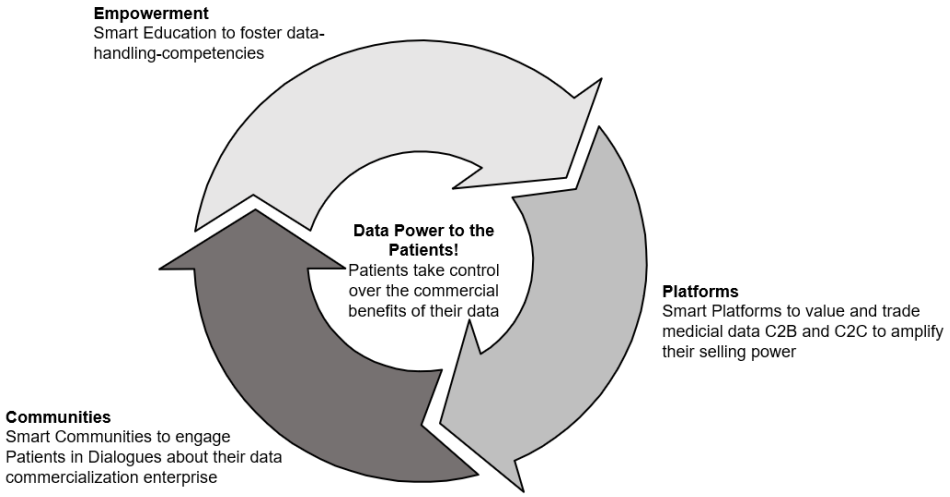

Figure 1: The centrality of the patient in the commerce of digital healthcare

IV. THE GDPR POTENTIALLY DRIVES THE INDIVIDUAL DATA BUSINESS IN MEDICINE

In my opinion, the General Data Protection Regulation (GDPR)[30] tries to manage the balancing act between data protectionism and innovation bondage in favor of a reasonable middle-of-the-range solution. It can – despite all certainly not unjustified criticism in detail – become the gold standard (for now) to make personal data with privacy and data portability a valuable asset in a seller's market. Businesses, as well as other public-sector institutions, for example, who deal with impersonalized data and, most importantly, personal data of patients, are highly demanded to ensure the maximum possible security of this data from misuse. Since like I mentioned true impersonalized data is not easy to grant, this form of data although not covered by the GDPR should be considered data protection relevant when we talk about patient data.

Additionally, it is a good initiative of the GDPR to put the consent clearly in the center. It is about protection people, not protecting data.[31] In the end, patients will have to learn

30 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504 (last visited Oct. 20, 2018, 04:26 PM).

31 The GDPR, in fact, is counterproductive when it comes down to the real business life. A little less complex, rigid and punitive might have been more suitable. In Germany things are, of course, even more complex. 18 independent data Protection authorities exist in Germany. Sometimes simplicity and clarity might be a better

to responsibly handle the most valuable data they have – their medical data – and to read the privacy policy. The "fine print" re-enters the consciousness – and that's a good thing. In addition, the much-cited informational self-determination is no guarantee of absolute power of the individual over "their" data – because also the protection of privacy takes place in a social context. And yet there remains the problem that the GDPR does not directly address the involvement of consumers in the economic exploitation of their data. It is easy to understand, however, that consumers want more than data protection as soon as the economic opportunities in data markets become clearer to them.[32] At the end of the day, it should be similar for patients – not just because of private return perspectives but also to foster their healthcare outcomes. Which on the other hand might also increase their motivation e.g. to share their data with research organizations and become a proud data donor. Precision medicine for everyone needs so many institutional barriers to overcome – Patients as smart customers can make it happen.

No sensible person can object to better medicine; however, care must be taken to ensure that there are no distorting data monopolies and non-transparent business models that in the end only really benefit a few players. If a legal, legitimate and efficient business is to emerge, it must properly engage patients as customers and data providers in the value chain. The centrality of the patient in the commerce of digital healthcare is crucial – also from my point of view for a holistic patient experience - even though it may be very complex and difficult, it is not impossible.

way to protect people and business as well as to help to avoid the misuse of their data than the current confusing legal framework. An international comparison of approaches is possible, e.g. the Hong Kong Personal Data (Privacy) Ordinance, the Australian Privacy Act, the Singapore Personal Data Protection Act etc. - for a good global overview check: *Data protection around the world*, DNIL, https://www.cnil.fr/en/data-protection-around-the-world (last visited Oct. 20, 2018, 04:31 PM).

32 Sarah Spiekermann & Jana Korunovska, *Towards a value theory for personal data*, 32 (1) JOURNAL OF INFORMATION TECHNOLOGY, 62-84 (2017).

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

COMPLIANCE AND VALUE ORIENTATIONS AT UNIVERSITIES

Melanie Wegel, Maria Kamenowski & Andrea Barbara Hartmann

AUTHORS

Melanie Wegel is project manager and lecturer at the Institute for Delinquency and Crime Prevention at the Zurich University of Applied Sciences in Switzerland. She holds a master degree and a PhD from the University Tübingen in Germany. Her focus of attention lays on prison and probation research and evaluation of projects concerning crime prevention.

Maria Kamenowski holds a master degree in Criminology from the University Regensburg in Germany. She works as a researcher in several projects at the Zurich University of Applied Sciences.

Andrea Barbara Hartmann holds a Bachelor Degree in Social Work and is employed at the Zurich University of Applied Sciences as a research assistant.

ABSTRACT

Compliance, defined as the obligation to follow particular rules[1] at the institutional level, can hardly be considered while disregarding individual actors: after all, it depends on the value orientation of their attitudes and actions.[2] Compliance with the law forms the basis for the actions of all companies, including universities. In Switzerland, most universities have no explicit compliance guides, but they often do have other guidelines that allow making statements about the identity of the institution. The Zurich University of Applied Sciences (ZHAW) has made social integration a priority for 2017/2018. Within the scope of this priority area, 13 research projects were funded; in this case, the subtopic was "work, diversity, living space and social security". In addition, the Department of Social Work provided ad hoc support for smaller projects that illustrate the aspect of social integration. Thus, this institution does not only set guidelines, but also actively promotes them. However, the question remains open as to whether the individual actors act and think in accordance with the guidelines of their institution. As part of a research project on value orientation[3]

---

1 AMITAI ETZIONI, A COMPARATIVE ANALYSIS OF COMPLEX ORGANIZATIONS: ON POWER, INVOLVEMENT, AND THEIR CORRELATES 33 et seq. (1961).

2 MILTON ROCKEACH, THE NATURE OF HUMAN VALUES (1973).

3 Project Nr. 162380 of the Swiss National Fonds, accessible at: http://p3.snf.ch/Project-162380 (last visited Apr. 26, 2018, 01:30 PM).

funded by the Swiss National Science Foundation, ZHAW employees were selected as a reference group and asked about their value orientation. The social factor being a crucial focal point at institutions of higher education, the survey was intended to show both the heterogeneity of the group and its common ground: the values shared by all the respondent members that are instrumental in guiding their actions. The precise manifestation of the respondents' social values was also of interest.

TABLE OF CONTENTS

I. COMPLIANCE AND VALUES: THE KNOWLEDGE BASE

Compliance, in a general sense of following certain rules, may occur in any social context in which people interact with each other.[4]
In business, compliance is understood to mean strategies that pursue the conformity to laws, as wells as regulations in the broadest sense.[5] In the following, we will refer to economics and organizational sociology; while we are aware that universities are not companies in the usual sense, they – at least the universities of applied sciences in Switzerland – are held economically accountable, being partly financed by providing services and attracting research funds. In this area, the observance of rules (even unwritten ones) is particularly important, forming as it does good scientific practice. If we take a closer look at the definitions of compliance from the perspective of economics, we see that in Roth's[6] understanding, for instance, the basis of compliance is a legal duty of companies to ensure that no violations of the law occur; however, the objective goes beyond this duty: compliance presumes not only that companies, i.e. their managers and all employees observe the laws but also that ethical standards shape the company's relationship to various stakeholder groups. In relation to economics, organizational sociology also deals with the issues of legal compliance in companies. Key issues in this context are compliance with rules as well as moral and ethical guidelines. Moral action is dictated by value orientations[7]; ethics are presently defined as principles that assume value-orientation as a norm for human action.[8]

In some cases, it is questionable whether social values agree or can be harmonized with organizational values, and how these possibly diverging values influence the actors. We may also ask whether value orientations may influence organizational goals and values. In economic processes, financial gains can often be more important than social values, and the pursuit of economic goals can lead enterprises into conflict with its declared social orientation.[9] An organisation's guidelines might also conflict with the individual values of its members. A crucial aspect of this conflict is information asymmetry: the official values of organisations are usually known; those of their members usually remain undisclosed. In the following, examples of compliance at Swiss universities will be discussed to shed light on the individual reflexive values of employees.

---

4 MITAI ETZIONI, A COMPARATIVE ANALYSIS OF COMPLEX ORGANIZATIONS: ON POWER, INVOLVEMENT, AND THEIR CORRELATES 3 et seq. (1961).

5 MONIKA ROTH, COMPLIANCE – VORAUSSETZUNG FÜR NACHHALTIGE UNTERNEHMENSFÜHRUNG. EIN BRANCHENÜBERGREIFENDES UND INTERDISZIPLINÄRES HANDBUCH MIT FALLSTUDIEN 17 (2016).

6 MONIKA ROTH, COMPLIANCE. IN A NUTSHELL 1-9 (2015).

7 Cf. Weber, 1922; cited after Pohlmann: MARKUS POHLMANN, SOZIOLOGIE DER ORGANISATION: EINE EINFÜHRUNG 166 (2016).

8 MARKUS POHLMANN, SOZIOLOGIE DER ORGANISATION: EINE EINFÜHRUNG 168 et seq. (2016).

9 MARKUS POHLMANN, SOZIOLOGIE DER ORGANISATION: EINE EINFÜHRUNG 168 et seq. (2016).

A. Discussing Compliance at Swiss Universities

While compliance is a central topic for business enterprises, it seems to receive less attention at universities. The scientific symposium "Compliance Management at Universities – More than Sticking to Rules" that took place in Germany in 2012 discussed this imbalance against the background of the increasingly complex regulations governing the university landscape: rules of conduct regarding such values as scientific integrity have come into focus.[10] Some universities have even published compliance concepts or guidelines. Some internal debate appears to be taking place at technical universities.[11] For Switzerland, information on compliance is only available under the heading "scientific/scholarly integrity".[12]

A detailed guideline explicitly called "Compliance Guide" can be found on the website of the Swiss Federal Institute of Technology (ETH) in Zurich.[13] The ETH Zurich defines compliance as pursuing its goals to strengthen integrity and independent action within the university. The definition also includes taking measures against all situations that could damage the reputation of ETH Zurich. The document is intended as a binding guideline for all members of the university across all departments; it relates to various areas such as finance, safety, health, the environment, research involving human subjects, etc. Normative principles such as federal laws, university ordinances and decrees as well as codes of conduct regarding values and ethics are taken into account.

In summary, it can be stated that there has been no discussion on compliance at universities to date, or at least no public discussion. While individual universities are dealing with this issue and developing tools, there seems to be no uniform concept. A striking aspect, though, are general statements of orientation that emerge as key themes or guidelines as well as codes of conduct for universities and individual departments. The importance of values is often addressed; however, the definition of these term often remains unclear.

---

10 FOM conference proceedings: Tagungsband Wissenschaftliche Fachtagung München, 22. – 23. November 2012. Compliance-Management an Hochschulen – Mehr als Regelkonformität (2013), https://link.springer.com/content/pdf/10.1007%2F978-3-658-01270-0_9.pdf (last visited Apr. 26, 2018, 10:48 AM)

11 Some examples are RWTH in Aachen, Germany (cf. Nettekoven 2012), ETH in Zürich, Switzerland (ETH 2015) or the School of Management of Law at ZHAW, also in Zürich (ZHAW 2012, 2018); ETH Compliance Guide (2015), https://rechtssammlung.sp.ethz.ch/Dokumente/133.pdf (last visited Apr. 26, 2018, 10:45 AM), ZHAW, Code of Ethics of the ZHAW School of Management and Law (2012, unpublished), and ZHAW, *Prinzipien für eine verantwortungsvolle Managementausbildung (PRME)* (2018), https://www.zhaw.ch/de/sml/ueber-uns/prme/ (last visited Apr. 26, 2018, 02:13 PM).

12 See, for example, Swiss Academies of Sciences, *Scientific Integrity. Compilation of codes of conduct: ZHAW, Dossier Wissenschaftliche Integrität* (2018), https://www.zhaw.ch/de/hochschulbibliothek/schreiben-publizieren (last visited Feb. 22, 2018, 09:56 AM).

13 ETH Zürich, Compliance Guide (2015), https://rechtssammlung.sp.ethz.ch/Dokumente/133.pdf (last visited Apr. 26, 2018, 01:23 PM).

B. Compliance and Value Orientation

In addition to the legal guidelines, compliance refers to values that are defined at a meso level by the organization; these are to be observed by the employees. As explained at the outset regarding compliance in economics, these values can be particularly relevant for behaviour in grey areas. If we define compliance as a behavioural concept and assume that employees are guided by values, the micro level also becomes relevant from the perspective of value research. After all, the individual value orientations of an organization's employees shape their attitudes and can have an impact on their behaviour. According to Rokeach,[14] values and value orientations have direct impact on behaviour; indeed, they are regarded as a motivational driving force for action. Value research shows that socialisation, value attitudes and normative orientations all influence the decision to conform to or deviate from certain values. In general, value means something desirable.[15] Individual reflexive values, the personal desires of individuals[16] shape lives and influence goals and actions.[17] Thus, values influence all aspects of action: the objectives, the means of achieving these objectives and the way in which the means are used. It is assumed that external living conditions go hand in hand with internal value orientations and behaviours.[18]

Careful consideration of employees' individual reflexive value orientations within a specific university can provide information about these orientations, the specific factors influencing them and the differences or similarities existing in the different disciplines.

C. ZHAW Guidelines

The ZHAW is a university of applied sciences in Switzerland that comprises eight departments: Applied Linguistics; Applied Psychology, Architecture, Design and Civil Engineering; Health; Life Sciences and Facility Management; School of Engineering; School of Management and Law; and Social Work. The employees work in teaching, research, development and further education, along with offering additional specialized services. ZHAW's long-term goals and annual guidelines can be cited as the documents describing the university's central values. The long-term value keywords are "knowledge-based and competence-oriented", "transformative" and "European". These goals were set for the next ten years in 2015. In addition, each year, ZHAW addresses key social challenges: for

14 MILTON ROCKEACH, THE NATURE OF HUMAN VALUES (1973).

15 Clyde Kluckhohn, *Value and value orientations in the theory of action, in:* Toward a general theory of action 388-433 (Talcott Parsons & Edward Shils eds., 1951).

16 DIETER HERMANN, WERTE UND KRIMINALITÄT. KONZEPTION EINER ALLGEMEINEN KRIMINALITÄTSTHEORIE 54 (2003).

17 MILTON ROCKEACH, THE NATURE OF HUMAN VALUES (1973).

18 DANIEL SEDDIG, SOZIALE WERTORIENTIERUNGEN, BINDUNGEN, NORMAKZEPTANZ UND JUGENDDELINQUENZ 94 (2014).

2017/2018, the focus is on energy and social integration. The focus of social integration can be directly related to the organization's values. Social values are key among modern idealistic values, and thus it made sense for ZHAW to actively concentrate on this aspect in 2017/18. For instance, "Social Integration" was a conference topic at a "Retraite"[19] organized by the Department of Social Work. Its aim was to develop projects that show how the university realizes the guiding principle of "social integration". Following this event, four projects were selected and implemented with financial support. One of these promoted the work integration of persons released from prison. Even more important was strengthening the field of social integration by means of research. In 2017, a call for proposals was launched, seeking research projects focusing on work, diversity, living space and social security. The objective of this initiative was a long-term implementation of the focus. 13 projects from a wide variety of disciplines were funded.[20]

ZHAW does not provide an explicit compliance guide, but it has drawn up several codes of conduct, such as the ZHAW Code of Ethics at the School of Management and LAW, which sets out the guiding ethical values such as respect and justice, integrity and trustworthiness, transparency and confidentiality, responsibility and sustainability. These apply to all activities of the ZHAW School of Management and Law, to all its employees and students.[21] The university is also involved in the UN initiative "Principles for Responsible Management Education" (PRME). PRME is an international network of over 650 researchers and universities from 65 countries that pursues the goal of "responsible management training", considering guiding principles of sustainability and presenting regular progress reports.[22] However, the personal value orientations of university employees remain largely unknown.

II. SAMPLE DESCRIPTION

The surveys among university employees were conducted online. ZHAW has a total of 2977 employees. The link to the online survey was sent to 1329 people; 735 of them completed the questionnaire fully or almost fully. Thus, almost 50% of the gross sample took

19 In Switzerland, a "Retraite" is a form of closed meeting attended by all employees of an organizational unit. This event takes place outside the institution and deals with a key topic.

20 Cf. ZHAW, *Forschungsschwerpunkt Gesellschaftliche Integration*, https://www.zhaw.ch/de/forschung/forschungsschwerpunkte/forschungsschwerpunkt-gesellschaftliche-integration/ (last visited Apr. 27, 2018, 09:36 AM).

21 Cf. ZHAW, *Forschungsschwerpunkt Gesellschaftliche Integration*, https://www.zhaw.ch/de/forschung/forschungsschwerpunkte/forschungsschwerpunkt-gesellschaftliche-integration/ (last visited Apr. 27, 2018, 10:25 AM).

22 ZHAW, *Prinzipien für eine verantwortungsvolle Managementausbildung (PRME)* (2018), https://www.zhaw.ch/de/sml/ueber-uns/prme/ (last visited Apr. 26, 2018, 11:56 AM).

part in the survey, which is considered a very good result for online surveys.[23]

In addition to structural data such as gender, age and nationality, the survey queried the duration of employment, the affiliation to a subject area and the religious denomination. To measure individual value orientation, we used an adapted form of the value scale by Klages extended by criminogenic values developed by Hermann[24] based on two representative questionnaires and a survey in a prison.[25] In addition, in accordance with the prison survey, university employees were also asked questions about the judicial system and punitive behaviour in Switzerland.

For all the following information, only those who made a statement in response to the respective question were included in the evaluation. 38.5 percent of the participants were male, and 61.5 percent female. Of the total of 6 age categories (from "under 24" to "over 60"), the median was the age category "41 to 50". Of the employees surveyed, around 83 percent said they were Swiss nationals. Most of the people surveyed had a university degree (around 75 percent); 35.7 percent of the respondents were administrative and/or technical personnel.

A. Key value orientations of university staff members

Value orientations can guide action and form behavioural strategies in private life as well as at work. Through an explorative factor analysis[26] with the items of the questionnaire's value scale, the dimensions were reduced to identify the most significant value orientations for the given sample. The procedure revealed two dimensions with a declared total variance of around 91 percent. According to the survey, the key values of ZHAW staff members are "aligning my life with religious norms and values" / "believing in God" with around 58 percent declared variance, and "having good friends who appreciate and accept you" with around 33 percent declared variance. Thus, the religious value orientation and the acceptance of friends form the common orientation for the sector of the employees: Gender and age are slightly related to these two dimensions. Women tend to ascribe crucial importance to "having good friends who appreciate and accept you" more often than

23 Online surveys are an effective and inexpensive way of collecting and entering data. The disadvantages are also obvious, though: we do not know if the link reached all addressees, and what the reason for non-participation or abandonment of the survey were.

24 Dieter Hermann, *Individuelle reflexive Werte. Zusammenstellung sozialwissenschaftlicher Items und Skalen* (2014), https://zis.gesis.org/skala/Hermann-Individuelle-reflexive-Werte (last visited Apr. 26, 2018, 01:31 PM).

25 The total scale contains three main theoretical dimensions: (1) traditional values, (2) modern idealistic values and (3) modern materialistic values. Cf: DIETER HERMANN, WERTE UND KRIMINALITÄT. KONZEPTION EINER ALLGEMEINEN KRIMINALITÄTSTHEORIE (2003).

26 Factor analysis is a method of dimension reduction. The aim is to find out which variables are central to the survey population. For the present study, factor analysis reduced the number of items to show more clearly what ZHAW employees understand by values. Main component analysis with Varimax rotation was selected for this purpose. Transverse charges were extracted if not uniquely loaded on a factor. The factor analysis procedure was carried out until a clear structure with the highest possible explanatory power emerged.

men (.149)[27], and older respondents tend to focus on "religious norms and values" more often than younger respondents (.130).

B. Age and gender

As noted previously, there is a weak link between gender and value orientation, which is in line with the general tendencies known from value research;[28] however, clear-cut divergences between age groups cannot be identified from the age categories available to us: the influence is rather weak. The median age category is "41 to 50". The central value orientations following from the factor analysis suggest that religion and friends matter to almost all respondents, thus forming their common denominator. In the following, we will show the variables influenced by the gender of the respondents.

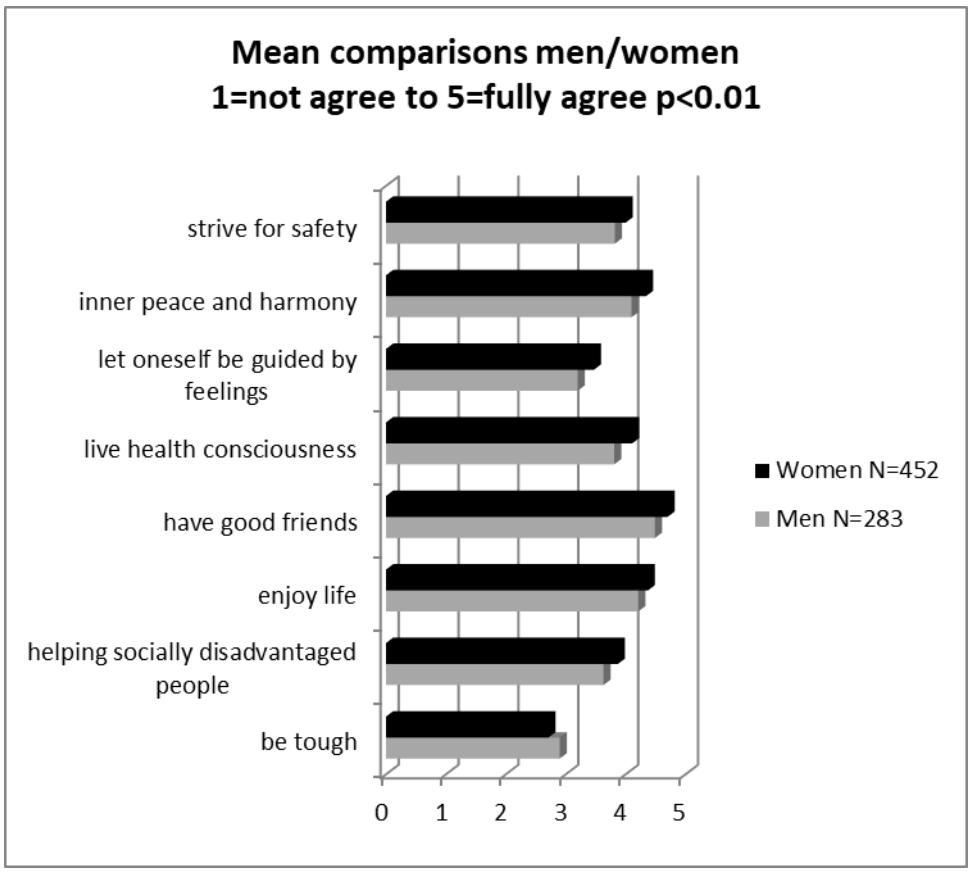

Figure 1.

27 The correlation coefficient is a measure of the degree of linear correlation between two at least interval-scaled characteristics. It can have values between - 1 and +1. If the value is 0, there is no connection.

28 DIETER HERMANN, WERTE UND KRIMINALITÄT. KONZEPTION EINER ALLGEMEINEN KRIMINALITÄTSTHEORIE (2003).

The figure only shows the significant differences in value orientations differentiated by gender. According to these data, security, inner peace and health matter more to women than to men. Women are more emotionally driven than men, and friends are even more important to them than to the male respondents. It is important for women to enjoy life and to help socially disadvantaged people. The final variable was not highly significant but is included in the analysis because it suggests that women tended to be more differentiated in their responses, considering the value of individual items closely rather than simply ticking the category "very important". "Hard and tough" is one of the criminogenic values from the Hermann 2003 value scale; it tends to be preferred by men rather than women[29]. Analysing the influence of sociodemographic factors in the value orientation in youth, Pöge also concluded that gender influences value orientation.[30] Since social integration is particularly important for the institution, the variable "helping socially disadvantaged groups" is exemplarily examined in more detail. By means of a regression analysis,[31] the variability of response to "helping socially disadvantaged groups" is explained mainly by gender, followed by age and finally by profession. Comparisons of the mean values do not give a clear picture here: members of the departments of Social Work, Health and Psychology and Linguistics rate the variable "helping socially disadvantaged groups" the highest, followed by members of the departments of Management and Law, as well as Engineering – but the differences are not always statistically significant. It is remarkable that the initiatives in the framework of the social integration guideline not only come from professions that traditionally have a close connection to social engagement – rather, the topic has met with great interest in all areas.

III. SUMMARY

In the educational field, the discussion of compliance is still in its infancy. Still, the guidelines and stated priorities of institutions merit attention: these often are de facto compliance statements in the broadest sense. ZHAW is an example of an institution whose priorities are not only well-considered but also actively implemented. The priority area "Social Integration", for instance, receives credibility and sustainability from the connection to research priorities, including the promotion of practical projects. A look at the employee level also shows considerable interest in social integration. Traditionally, such a focus is considered easier to implement in professions committed to the social realm than in the technical and other professions – however, our study shows that characteristics such as gender and age offer more explanatory power than professional self-identification.

29 Melanie Wegel/Anna Isenhardt/Maria Kamenowski, *Geschlecht und Delinquenz: Die Wertetheorie und ihr Erklärungspotenzialmit Blick auf weibliche Inhaftierte*, 30 (2) NEUE KRIMINALPOLITIK, 189 – 209 (2018).

30 ANDREAS PÖGE, WERTE IM JUGENDALTER (2017).

31 The model was significant overall: Durbin Watson 1.92.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

ELIMINATING BRIBERY - AN INCENTIVE-BASED APPROACH

Fabian M. Teichmann

AUTHOR

Fabian M. Teichmann is an Attorney-at-Law and Public Notary whose area of research interest centers on corruption, money laundering and the financing of terrorism. After having pursued an undergraduate degree in economics and finance from Bocconi University, he earned graduate degrees in management from Harvard University and in law as well as in accounting and finance from the University of St. Gallen. In addition, Fabian Teichmann holds a PhD in law from the University of Zurich and a Doctor of Economics and Social Sciences from the University of Kassel. Today, he runs a Swiss law firm and consulting companies in England, Liechtenstein and the United Arab Emirates. In his free time, he teaches courses on "Compliance in Multinational Corporations".

ABSTRACT

This article discusses the potential role of incentive systems in combating bribery. In particular, it uses an agency theory approach to show how a combination of bonus and malus payments could help to eliminate bribery in multinational corporations. Expert interviews with 35 anti-bribery specialists from Austria, Germany, Liechtenstein, and Switzerland were conducted and analyzed through qualitative content analysis. It was found that employees should be rewarded for both productivity and compliance. In addition, performance should be measured in a matrix and whistleblowers should receive a bonus for reporting undesired behavior. Conversely, significant risks associated with incentives for whistleblowing were also identified. Whilst the empirical findings focus on Europe, their implications could be applied globally.

TABLE OF CONTENTS

I. INTRODUCTION

Twenty years ago, bribery was still commonly accepted in many areas of the world. However, corruption leads to inefficient use of resources, unfair redistribution of income, and secessionist responses.[1] Frustration, unstable sociopolitical situations, and a lack of contentment among private citizens are just a few of the potential outcomes.[2] In addition, bribery requires secrecy, which makes the enforcement of agreements very difficult.[3] Given its many negative impacts on a country's development, multiple nations have outlawed bribery.[4]

However, bribery has not yet been eliminated, with multiple attempts to combat this phenomenon ultimately failing. This article will present an agency theory-based approach towards eliminating bribery. In particular, it will analyze and discuss whether incentive systems could be adjusted to more effectively fight bribery in multinational corporations, thereby helping to decrease corruption in developing countries.

II. LITERATURE REVIEW

For this study's purpose, the bribery definitions of the OECD Anti-Bribery Convention and Transparency International are amalgamated to define bribery as an act in which a party:

> *intentionally abuses entrusted power for private gain by offering, promising, or giving any undue pecuniary or other advantage, whether directly or through intermediaries,*

---

1 Mark Levin & Georgy Satarov, *Corruption and institutions in Russia*, EUROPEAN JOURNAL OF POLITICAL ECONOMY, 16(1), 113, 114f. (2000); Antonio Argandoña, *The United Nations convention against corruption and its impact on international companies*, JOURNAL OF BUSINESS ETHICS, 74(4), 481, 482 (2007); Michael W. Collier, *Explaining corruption: An institutional choice approach*, CRIME, LAW AND SOCIAL CHANGE, 38(1), 1, 6(2002).

2 Christopher J. Anderson & Yuliya V. Tverdova., *Corruption, political allegiances, and attitudes toward government in contemporary democracies*, AMERICAN JOURNAL OF POLITICAL SCIENCE, 47(1), 91 , 104 (2003); Pak Hung Mo, *Corruption and economic growth*, JOURNAL OF COMPARATIVE ECONOMICS, 29(1), 66, 67 (2001); Jong Bum Kim, *Korean implementation of the OECD bribery convention: Implications for global efforts to fight corruption*, UCLA PACIFIC BASIN LAW JOURNAL, 17(2/3), 245, 249 (1999).

3 Paolo Mauro, *Why worry about corruption?*, ECONOMIC ISSUES 6. WASHINGTON, D.C.: INTERNATIONAL MONETARY FUND, 6 (1997); Pranab Bardhan, Corruption and development: A review of issues. JOURNAL OF ECONOMIC LITERATURE, 35(3), 1320, 1320 (1997); Paolo Mauro, *The effects of corruption on growth, investment, and government expenditure*, IMF WORKING PAPER, WP/96/98 WASHINGTON, D.C.: INTERNATIONAL MONETARY FUND, 86 (1996); John Bray, *The use of intermediaries and other alternatives to bribery, in*: The new institutional economics of corruption, 120(Johann Graf Lambsdorff, Markus Taube & Matthias Schramm eds., 2005).

4 Hongyi Li, Lixin Colin Xu & Heng-fu Zou, *Corruption, income distribution, and growth*, ECONOMICS & POLITICS, 12(2), 155, 156 (2000); Aart Kraay, Pablo Zoido-Lobaton & Daniel Kaufmann, *Aggregating governance indicators,* POLICY RESEARCH WORKING PAPER 2195 WASHINGTON, D.C.: WORLD BANK, 3 (1999).

> *to a foreign public official, for that official or for a third party, in order that the official act or refrain from acting in relation to the performance of official duties, in order to obtain or retain business or other improper advantage in the conduct of international business.*[5]

This definition is ideal for this study since countries throughout the world have based their national legislation on the OECD Anti-Bribery Convention. Moreover, Transparency International's definition is the approach employed in the best-known corruption index.

This study employs an agency theory approach. In particular, it will emphasize that "principals" and "agents" have differing interests[6], and that the former commonly desire to be compensated for acting in accordance with the latter's best interests.[7] Ultimately, principals bear responsibility for the outcome of a task delegated to their agents.[8] This is particularly problematic if agents are unsupervised[9], in which circumstance they might shirk or use the corporation's resources for their own benefit.[10] This constitutes a significant challenge as regards bribery, which is commonly conducted secretly, such that shareholders and CEOs (principals) may not always be aware of actions taken by the company's sales managers (agents). In this context, incentives could potentially prevent employees from simply reducing their risk and forcing the owners to bear a bigger share of it.[11] Of course, internal audits and control mechanisms could be used simultaneously to address agency problems.[12]

However, the use of incentives to fight bribery has not yet been investigated in depth.

---

5 See *FAQs on corruption,* December 20, 2015, TRANSPARENCY INTERNATIONAL, http://www.transparency.org/whoweare/organisation/faqs_on_corruption (last visited 10 Oct. 2018), 1 (2015); OECD, *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and related documents*, 6(4), OECD WORKING PAPERS, https://www.oecd.org/daf/anti-bribery/ConvCombatBribery_ENG.pdf (last visited 10 Oct. 2018), 7 (2011).

6 Kathleen M. Eisenhardt, *Agency theory: An assessment and review*, ACADEMY OF MANAGEMENT REVIEW, 14(1), 57, 59 (1989).

7 Patrick McColgan, *Agency theory and corporate governance: A review of the literature from a UK perspective*, 6 (2001).

8 Stephen A. Ross, *The economic theory of agency: The principal's problem*, THE AMERICAN ECONOMIC REVIEW, 63(2), 134, 134 (1973)

9 Peter Wright, Ananda Mukherji & Mark J.Kroll, *A reexamination of agency theory assumptions: Extensions and extrapolations*, THE JOURNAL OF SOCIO-ECONOMICS,30(5), 413, 426 (2001).

10 Luis R. Gomez-Mejia & David B. Balkin, *Determinants of faculty pay: An agency theory perspective*, ACADEMY OF MANAGEMENT JOURNAL, 35(5), 921, 923 (1992).

11 Henry L. Tosi, Jr. & Luis R. Gomez-Mejia, *The decoupling of CEO pay and performance: An agency theory perspective*, ADMINISTRATIVE SCIENCE QUARTERLY, 34(2), 169, 169 (1989).

12 Michael B. Adams, *Agency theory and the internal audit*, MANAGERIAL AUDITING JOURNAL, 9(8), 8, 12 (1994).

The overwhelming majority of literature on wages and bribery has focused on the public sector and on adequate wages in general, rather than on incentives.[13] For instance, it has been analyzed whether tax collectors openness to bribery may be increased by using incentive systems.[14] It has also been discussed whether graders in Burkina Faso are more or less likely to accept bribes under bonus or malus systems.[15] In contrast to previous studies, this article will analyze whether incentive systems could help to eliminate bribery in multinational corporations.

III. METHODY

Due to the significant research gap identified above, it was not possible to form hypotheses that could be quantitatively tested. Therefore, an explorative approach was chosen.[16] Thirty-five formal interviews were conducted with anti-bribery experts from Austria, Germany, Liechtenstein, and Switzerland, aiming to answer the following research questions:

> *How could incentive systems help to prevent corruption in multinational corporations?*
>
> *Which risks are associated with anti-bribery incentives?*

The interviewees were recruited through the author's personal network, and the interviews were transcribed and analyzed using qualitative content analysis.[17] The recruited interviewees have various backgrounds. First, 15 white-collar criminals were interviewed in

---

13 Rajeev K. Goel & Daniel P. Rich, *On the economic incentives for taking bribes*, PUBLIC CHOICE, 61(3),269, 269f. (1989); Rafael Di Tella & Ernesto Schargrodsky, (2003). *The role of wages and auditing during a crackdown on corruption in the city of Buenos Aires*, JOURNAL OF LAW AND ECONOMICS, 46(1), 269, 269f. (2003); Gary S. Becker & George J. Stigler, *Law enforcement, malfeasance, and compensation of enforcers*, THE JOURNAL OF LEGAL STUDIES, 3(1), 1, 6 (1974); Caroline Van Rijckeghem & Beatrice Weder, *Bureaucratic corruption and the rate of temptation: Do wages in the civil service affect corruption, and by how much?*, JOURNAL OF DEVELOPMENT ECONOMICS, 65(2), 307, 307 (2001).

14 Timothy Besley & John McLaren, *Taxes and bribery: The role of wage incentives*, THE ECONOMIC JOURNAL, 103(416), 119, 137 (1993); Dilip Mookherjee, *Incentive reforms in developing country bureaucracies: Lessons from tax administration, in:* Annual World Bank Conference On Development Economics, 103 (Boris Pleskovic & Joseph. E. Stiglitz eds., 1997).

15 Olivier Armantier & Amadou Boly, *On the effects of incentive framing on bribery: Evidence from an experiment in Burkina Faso*, ECONOMICS OF GOVERNANCE, 15(1), 1, 13 (2014).

16 Robert M. Bowen, Andrew C. Call & Shiva Rajgopal, *Whistle-blowing: Target firm characteristics and economic consequences*, THE ACCOUNTING REVIEW, 85(4), 1239–1271 (2010); Kevin Buckler, *The quantitative/qualitative divide revisited: A study of published research, doctoral program curricula, and journal editor perceptions*, JOURNAL OF CRIMINAL JUSTICE EDUCATION, 19(3), 383–403 (2008); JOHN W. CRESWELL, RESEARCH DESIGN: QUALITATIVE, QUANTITATIVE, AND MIXED METHOD APPROACHES 183 (4th ed., 2013).

17 PHILIPP MAYRING, QUALITATIVE INHALTSANALYSE: GRUNDLAGEN UND TECHNIKEN, 10f (11th ed., 2010).

order to understand the perspective of those committing bribery. Subsequently, 20 prevention and law enforcement experts were interviewed. Eight interviewees were recruited from big four consulting firms prominent in the field of anti-bribery compliance in multinational corporations. This allowed particular focus on fraud investigation and dispute services. Eight compliance officers of multinational corporations, responsible for designing and implementing anti-bribery policies, were also interviewed. Finally, four law enforcement experts were interviewed. In analyzing the interviews, a category system was formed and assessed on its objectivity, reliability, and validity through triangulation. [18]

IV. EMPIRICAL RESULTS

According to the partners of the big four consulting firms, both productivity and compliance should be remunerated, since employees are expected to be productive and act compliantly. By only paying them for productivity, employees may seek non-compliant ways of increasing their output. In this context, current incentive systems may even encourage employees to break compliance rules.

However, the compliance officers in multinational corporations contended that rewarding both productivity and compliance can be rather challenging, given the difficulty of determining whether an employee has acted compliantly or not. Therefore, it is important to use performance matrixes that include several types of output.

The partners of the big four consulting firms also suggested introducing a bonus and malus system, as well as a bonus bank. Employees could then be rewarded for productivity and compliance, with small compliance violations (those that are not grounds for terminating employment) resulting in a malus deduction from their bonus bank. This could help to partially overcome the lack of transparency commonly associated with bribery, since acts of non-compliance may be discovered several years after their commission. Bonus banks could, thus, help to ensure that employees paying bribes are not rewarded economically for their actions.

The white-collar criminals suggested rewarding whistleblowing as an additional control mechanism. The underlying reasoning is that employees (agents) can control one another but need an incentive to be willing to report their peers. Hence, a bonus could be paid for whistleblowing.

Conversely, the compliance officers emphasized that bonus payments for whistleblowing could lead to false accusations and, hence, unnecessary investigations. In addition, such

---

18 Marilyn Healy & Chad Perry, *Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm*, QUALITATIVE MARKET RESEARCH, 3(3), 118, 118f (2000).; Nicholas Mays & Catherine Pope, *Assessing quality in qualitative research*, BRITISH MEDICAL JOURNAL, 320(7226), 50, 50 (2000); Janice M. Morse, Michael Barrett, Maria Mayan, Karin Olson & Jude Spiers, *Verification strategies for establishing reliability and validity in qualitative research*, INTERNATIONAL JOURNAL OF QUALITATIVE METHODS, 1(2), 13, 13f (2002).

whistleblowing bonuses could have a negative impact in team-based cultures, since people could stop trusting one another.

V. CONCLUSION

Incentive systems could play an important role in eliminating bribery. In particular, employees should be rewarded for both productivity and compliance, with performance measured through matrixes. In addition, a combination of bonus and malus payments could help to reward compliant and sanction non-compliant behavior. Bonus payments for whistleblowing could also help to establish an additional control mechanism. In this context, however, it should be kept in mind that whistleblowing bonuses could lead to false accusations and destroy the team-based cultures central to many corporations. Finally, it should be recognized that a study with a larger sample conducted in different countries or at a different time could produce different results.[19]

19 Janice M. Morse, Michael Barrett, Maria Mayan, Karin Olson & Jude Spiers, *Verification strategies for establishing reliability and validity in qualitative research*, INTERNATIONAL JOURNAL OF QUALITATIVE METHODS, 1(2), 13, 18 (2002); FABIAN M. TEICHMANN, ANTI-BRIBERY COMPLIANCE INCENTIVES, 10f (2017).

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

BOOK REVIEW

LEGAL UPHEAVAL: A GUIDE TO CREATIVITY, COLLABORATION, AND INNOVATION IN LAW

Michele DeStefano, Ankerwycke, Chicago 2018
ISBN: 9781641051200

Reviewed by Hendrik Schneider

AUTHOR

Hendrik Schneider, Founder and Content Curator of CEJ, is presently the head of the department of Criminal Law, Criminal Procedure, Criminology, Juvenile Law, and Sentencing at the University of Leipzig Faculty of Law. His current practice includes serving as legal counsel on corporate- and medical- criminal cases and advising on criminal matters surrounding issues of economic transactions and forensic investigations. Additionally, he acts as a compliance consultant with particular emphasis on the healthcare industry, including risk analysis, development and implementation of internal guidelines, change management, employee training, and sustainable protection.

REVIEWED BOOK

Founder and Content Curator of CEJ, Michele DeStefano recently published her new book Legal Upheaval: A Guide to Creativity, Collaboration and Innovation in Law, adressing the overthrow in the market for legal services and the associated challenges for the sector. Michele DeStefano is the founder and director of LawWithoutWalls and a Professor of Law at Miami Law. She is an expert in entrepreneurship in the law. Her scholarship focuses on the growing intersections between law and business and legal entrepreneurship.

A few weeks ago, I was finally able to hold in my hands the book of my colleague, friend, and co-founder of the CEJ, Michele DeStefano. I read it almost from top to bottom in one go, with great pleasure and with the highest appreciation.

At a meeting in Berlin, Michele, still in the middle of her creative process, explained to me that her book was about the "innovation tournament"[1] in the legal consulting market. The result, if one wants to assign it to the established genres of legal literature, cannot fit into any category. The empirical core of the paper consists of over 100 quality interviews from "GCs and chief executives from large international organizations along with heads of innovations and law firm partners from around the world"[2].In terms of methodology, DeStefano builds on her previous papers[3] and inductively develops statements regarding the self-perception and external perception of cooperation between law firms and their clients from industry and business. The result of such analyses is an innovative paper in the area of law and sociology regarding the legal professions and the demands placed on them by their corporate clients. However, the paper also gives specific recommendations regarding change management in the legal marketplace[4] in the form of a "cookbook" and regarding the adaptation of products and the billing (pricing) of services provided by law firms to the changing needs of effective legal consulting.

DeStefano succeeds in combining scientific substance and practical relevance and presenting her findings in an exciting, intuitive narrative style. The paper breaks new ground with the question that is pursued and with the scientific approach, as the analysis regarding the compatibility of the services provided by law firms with the needs of their clients is grounded empirically for the first time, and the paper makes visible and documents the connections that were previously surmised and felt, but not scientifically structured and documented, by the actors on the legal market.

The theoretical frame of reference of the paper consists of a reconstruction of the social, legal, and economic environment of the legal market.[5] Changes to this environment create a situation of pressure for law firms, rendering inevitable an adaptation and reorientation

---

1 p. 20 et seq, page references here and below refer to MICHELE DESTEFANO, LEGAL UPHEAVAL: A GUIDE TO CREATIVITY, COLLABORATION, AND INNOVATION IN LAW (2018).

2 p. 217.

3 Michele DeStefano, *Creating A Culture Of Compliance: Why Departmentalization May Not Be The Answer*, 10 (1) HASTINGS BUSINESS LAWJOURNAL, 71 et seq. (2014).

4 p. 157 et seq.

5 p. 3 et seq.

of legal advisory services, along with a redefinition of the relationship between the corporate client and the external law firm ("innovate or die"[6]). DeStefano identifies three factors of influence or forces that generate such pressure to innovate. Technology (for example, artificial intelligence, blockchain) means that certain standardizable services (drafting of a contract, prediction of the chances of success of proceedings, etc.) no longer have to be developed or worked out by attorneys "by hand"; rather, such technology may be available on demand within the framework of digital solutions. This changes the price structure of the products and the manner in which they are commissioned and called up. DeStefano illustrates this with the examples of copyright registrations and trademark filings[7], which can be undertaken today more cost-effectively and more rapidly without an attorney through the services of specialized providers of technical solutions. This translates into a change in demand for traditional consulting and requires a differentiation between services that can be provided with the assistance of technology or solely through technology, and those that require personal legal consulting and problem solving. As the second driver of change, the author refers to socio-economic and demographic changes, which will not stop with the future clients of law firms. Digital natives will confront advisory law firms with requirements regarding communication, teamwork, technology, etc. that are different than those of the "workforce traditionalists" or "baby boomers" generations (p. 7). The third factor of influence is the evolution of legal material, which can be observed around the world and is of increasing importance, as legal issues often have references both to local law and to the law of other nations and legal cultures. The pitfalls that can occur in international internal investigations provide an example of this,[8] because a variety of issues in areas of labor law, criminal law and data protection must be identified and managed ("globality and glocality"[9]).

The responses of GCs, to which DeStefano refers in her section entitled "the lawyer skills delta," indicate that the needs of GCs in the companies seeking legal assistance are often not adequately met by the commissioned attorneys. The requirement profile consists of an "end-to-end solution." An interviewee[10] describes this as "the optimal combination of people, process, tools and technology, and hybrid inside / outside sourcing models, to meet their client's business and legal challenges." Accordingly, profound legal expertise is merely a basic requirement to meet the requirements of clients. For this reason, the narrower sense, DeStefano does not even count such technical qualifications among the three levels, from the basis of satisfactory performance up to best practice with an "ecstatic client." In a legal environment that DeStefano rightly describes, in the style of Cold War

6 p. 133.

7 p. 12.

8 Hendrik Schneider, *The Enterprise in Testudo Formation*, 3(1) CEJ, 43 (2017); p. 50 et seq.

9 p. 8 et seq.

10 p. 34.

military terminology, as "VUCA" (volatile, uncertain, complex and ambiguous[11]), the external legal adviser should offer solutions and directions, and not simply point out problems. Anyone who is already drowning in e-mails[12] does not need a paper mountain or "over the top legal advice"[13]; rather, such person needs a strategic partner with empathy and the right answers for the task to be accomplished together.

However, it must also be mentioned that this also depends on the specific task with regard to the depth of content and the scope of the consulting service. A "hedged report" that legally assesses a particular transaction and is intended to serve as argumentative substantiation in (future) criminal or civil proceedings follows premises different than legal advice within the framework of an in-house process, such as advising an e-health start-up, which collects data in compliance with the law and wants to bring to market innovative medical devices for smart diagnostics around the world.

Furthermore, the qualitative interviews make it very understandable that the differentiation of the legal material often compels cooperation in a team of multiple specialists. This distinguishes GCs from their external consultants. While the former are often legal generalists, who have broad basic knowledge in various legal matters, external expertise is acquired on special issues. In an interview with a law firm based in New York, one partner says "I know a whole lot of a tiny area of law"[14]. This depth of knowledge is required to provide the desired legal information quickly, confidently and accurately. However, constructive cooperation with other experts within and outside the consulting firm is required to successfully manage the entire project. As such, in the innovation tournament, only a person who has expertise in "collaborative creative problem finding and solving" can assert himself or herself[15].

The author is aware that it is not only the case that such expertise is often neither reflected nor promoted in the workplace; it is also neglected in traditional legal education. With the worldwide university program LawWithoutWalls,[16] as she brings it to life, she has succeeded in closing this gap, occupying the interface between law, business and technology, and supporting students in building up the key interdisciplinary qualifications necessary to support the drive to innovate ("building collaborative relationships"). DeStefano successfully applies the know-how gained in this process in the design of the innovation process ("regardless of the size or location of your firm or legal department"[17]).

---

11 p. 10.

12 p. 39.

13 p. 50.

14 p. 10.

15 p. 49.

16 see Appendix B, p. 214 et seq.

17 p. VI.

The entire paper is so motivating and full of inspiration and new ideas that it is immediately contagious. The reader will want to put into effect what Michele DeStefano describes and teaches, both at the university and in the practice of legal consulting. Congrats, Michele, particularly for the many quotes and examples that will stay in my mind and surely the minds of other readers - from the "Man in the Mirror"[18] to "Mr. Wolf" in "Pulp Fiction"[19].

18 p. 56.

19 p. 64.